1-24-2024

Effective Strategies University Information Technology Leaders Use to Prevent or Mitigate Cyberattacks’ Costs

Rene Ekoteson
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Rene Ekoteson

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Irene Williams, Committee Chairperson, Doctor of Business Administration Faculty

Dr. WooYoung Chung, Committee Member, Doctor of Business Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2024

Abstract

Effective Strategies University Information Technology Leaders Use to Prevent or Mitigate Cyberattacks' Costs

by

Rene Ekoteson

MS, Wilmington University, 2016

BS, University Dschang, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

January 2024

Abstract

Cyberattacks pose a significant threat to university institutions as universities increasingly rely on computer networks to conduct day-to-day business activities. University information technology (IT) leaders are concerned about the increasing level of cyberattacks because these attacks can result in the loss of sensitive data, identity theft, and derivative costs. Grounded in systems theory, the purpose of this qualitative pragmatic inquiry was to explore strategies IT leaders of universities in Cameroon use to prevent or mitigate the costs of cyberattacks. The participants were eight IT leaders of universities in Cameroon with at least five years of experience in cybersecurity management and who successfully implemented effective strategies to prevent or mitigate the costs of cyberattacks. Data were collected using semistructured interviews and analyzed using thematic analysis. Three key themes emerged: employing multiple strategies to prevent or mitigate the cost of cyberattacks, incorporating educational training programs, and adopting security policies and procedures for best practices to ensure business continuity. A key recommendation is for university IT leaders to conduct regular cybersecurity awareness training, focusing on patient prevention, password security, and engineering social engineering awareness. The implication for positive social change is the potential to enhance cybersecurity measures and improve business viability and job creation, positively impacting the local communities and tax revenues.

Effective Strategies University Information Technology Leaders Use to Prevent or Mitigate Cyberattacks' Costs

by

Rene Ekoteson

MS, Wilmington University, 2016

BS, University Dschang, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

January 2024

Dedication

I dedicate this dissertation to my mother, Fanny Epote. My Father, Peter Ekote; My grandmother, Julie Nsulie, Ebwelle Jerry, Helen Ekoteson, Patricia Smith; and my two beautiful daughters, Shannell and Shaleen, supported me. I know for sure that I will continue to do so. This journey was a challenging process in my life. I dedicate this dissertation to my brothers Ramsey Ekote, Ajah Ekote Ajango, Chief Ekote, Ekwelle Ekote, and Ekiti Mactony. My sisters Doris Mbulle and Irene Dione. My friends Eric Kwene, Nelson Ngulle, and Dr. Joe Ngalle. Thank you all for your support and encouragement. Above all, I dedicate this dissertation to the synagogue church of all nations. Thank almighty God for giving me the wisdom and strength to make this journey successful.

Acknowledgments

I express my heartiest gratitude to my Chair, Dr Irene Williams. Thank you for your mentorship. This project would have never seen the brightness of the day without your scholarly and thoughtful comments. I would also like to thank my committee members, Dr. Edgar Jordan and Dr. Wooyoung Chung, for their generous advice, support, and encouragement throughout this study. This journey could not have progressed without the generous help of the participants. I would like to acknowledge the participants in this study who offered me their valuable time and knowledge.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Cyberattacks against academic institutions continue to incapacitate educational growth because of attacks on institutional and personal data. Academic institution leaders are under pressure to prevent cyberattacks (Fouad, 2021). Cyberattacks progressively damage networks and systems and are universally growing in number and severity (Rakas et al., 2020). The fact that academic institutions hold staff and students' sensitive data and depend on information systems in daily activities makes them prime targets for cyberattacks. However, educational institutions often lack the essential resources to deploy emerging cybersecurity methods and exploit business opportunities (Shlomo et al., 2021). This study was conducted to identify and explore effective strategies IT leaders of universities in Cameroon use to prevent or mitigate cyberattack costs.

This section gives a general overview of this study and the problem addressed therein. The remainder of Section 1 comprises the background, the business problem, and the purpose that explains the study's intent. This section includes the study population and sampling, the method and design for the study, the research questions, the conceptual framework, the significance of the study, a list of relevant definitions of terms used in this study, and the assumptions and limitations of this study.

Background of the Problem

Cybersecurity is a global concern, and organizations everywhere need solutions that work for them. In recent years, many new and evolving cybersecurity threats have put the worldwide information security industry on security alert (Shlomo et al., 2021). Intellectual cyberattacks involving malware, phishing, machine learning, artificial intelligence, cryptocurrency, and others have placed the data and assets of businesses, governments, and individuals at constant risk (Shlomo et al., 2021). For example, in April 2011, Sony had a PlayStation Network attack, Equifax had a March 2017 data breach with more than 145.5 million accounts compromised, and as a result of evidence linking Russia's interference in the United States election campaign, the U.S. government remains on security alert (Alraja et al., 2023). Marriott International also suffered a massive data breach in the United Kingdom in 2016, affecting as many as 500 million guests (Peterson et al., 2022). In 2017, in Cameroon, a country in the sub-Saharan African region, a cybersecurity student hacked 10 government websites overnight (Boraine & Doris, 2019). From 2015 to 2017, five cybersecurity incidents occurred in universities in Cameroon (Kessi et al., 2020).

Prior researchers have focused on the cybersecurity concerns of typical Western organizations. For example, Whitman and Mattord (2022) examined information security management in small enterprises in the United States and found that acceptable security compliance practices, implementation of security policies, and security awareness were significant countermeasures for preventing cyberattacks. Alraja et al. (2023) researched cybersecurity in higher education in Colorado and found that due diligence and oversight controls are central to securing a technological environment alert. Har et al. (2022) conducted an exploratory analysis of information security management in Australian universities. Har et al. developed a security management model to facilitate the transition of expert security practitioner knowledge into implementation.

The governmental structure of Cameroon is a notable factor that one must consider when studying or exploring cybersecurity management in this country. A country's unique cultural, political, and legal systems may alter how leaders of organizations manage cybersecurity. The prevailing view among citizens is that laws are mere formalities. The inhabitants in Cameroon view regional and local rules as more relevant and valuable than national-level laws and regulations. Regional and local provisions supersede national-level laws and regulations (Kessi et al., 2020). Cameroon is bicultural and bilingual because of the prolonged colonial administration of the British and French. Cameroon gained independence in 1961, less than six decades ago. Based on the colonial legacies, Cameroon's various systems of practice convey its dual cultural and linguistic colonial background (Kessi et al., 2020).

Cameroon's unique cultural, economic, and political system significantly influences how IT leaders implement cybersecurity controls to prevent emerging cyberattacks in Cameroon. Cameroon is a developing country lacking resources and technology, and Cameroon's unique cultural, political, and legal systems affect universities more than typical organizations. The universities are owned and controlled by the government. The government has more influence on how university administrators and security managers manage cybersecurity activities in their institutions (Kessi et al., 2020). University institutions are becoming political targets and vulnerable to cyberattacks because the government controls them. The Cameroon educational sector operates in two subsystems, the French and the English systems, with diverse curricular, structural, and organizational patterns. Allocating resources to cybersecurity should be a top priority of any manager. But universities' IT leaders lack the resources and the necessary technology to fight against cyberattacks (Kessi et al., 2020). Therefore, my objective in this study was to explore strategies that IT leaders of universities in Cameroon use to prevent or mitigate the costs of cyberattacks.

Problem and Purpose

Cyberattacks pose a significant threat to university institutions as universities increasingly rely on computer networks to conduct day-to-day business activities (Tayaksi et al., 2022). Cyberattack incidents increased by 125% through 2020, and increasing volumes of cyberattacks continued to threaten businesses and individuals in 2021 (Al-Ghamdi, 2021). Globally, 79% of business organizations have not developed a response strategy to cyberattacks (Tayaksi et al., 2022). The general business problem was that university institutional leaders faced a rising risk of cyberattacks that could result in increased loss of sensitive data, identity theft, and derivative costs. The specific business problem was that some information technology (IT) leaders in Cameroon universities lack effective strategies to prevent or mitigate cyberattack costs.

The purpose of this qualitative pragmatic inquiry was to explore the effective strategies IT leaders of universities in Cameroon use to prevent or mitigate cyberattack costs. This study’s population comprised eight IT leaders from universities in Cameroon with more than 5 years of experience in cybersecurity management and used effective strategies to prevent cyberattacks. IT leaders were suitable participants for this study because of their knowledge and experiences in preventing and mitigating cyberattacks. This study’s findings could be valuable to IT leaders and cybersecurity professionals to plan and implement effective strategies to prevent cyberattacks. This study’s findings may contribute to a positive social change by giving university IT leaders confidence and the necessary procedures to safely secure students' and staff's sensitive data and improve the economy's health. Furthermore, positive social change can result from providing a safe and secure learning environment for universities to conduct daily business activities.

Population and Sampling

This study's population comprised IT leaders, IT managers, and chief information officers (CIOs) in universities across Cameroon. This study's participants were eight IT leaders, IT managers, and CIOs with at least 5 years of experience in cybersecurity management. These participants were significant in addressing the research problem because universities assume abundant information security policy compliance. IT leaders such as security managers contributed to this study because they manage cybersecurity functions in their respective institutions. To participate in this study, the individual had to be an IT leader with at least 5 years of experience in cybersecurity management and must have used effective strategies to prevent cyberattacks. The participant also needed to be 25 or older. I used purposeful sampling to recruit participants familiar with what the university has done for cybersecurity. I continuously selected participants until I reached enough agreeable participants to meet the determined sample size and achieve data saturation. Six participants per group is recommended minimum number to enter the data saturation point in a typical qualitative study (Creswell & Creswell, 2018).

Nature of the Study

The research methods researchers use include qualitative, quantitative, and mixed methods (Yin, 2018). I used the qualitative method for this study. Researchers use the qualitative approach to describe the phenomena under study (Hamilton & Finley, 2019). The qualitative method was suitable for this study because I sought to identify and explore effective strategies that Cameroon university IT leaders used to prevent or mitigate the costs of cyberattacks. A qualitative approach is appropriate when a thorough understanding of an issue is necessary (Andrews, 2021). Addressing the research question required an in-depth analysis of the participants' experiences. The qualitative approach was appropriate for this study because it enabled the researcher to gather participant data through individual interviews. In contrast, researchers use the quantitative method to test hypotheses or examine the relationships among variables (Huyler & McGill, 2019), which was unsuitable for this study. Researchers use the mixed method when the research question, objective, and context require hypothesis testing and an in-depth analysis of participants' experiences (Sim, 2020). The mixed method approach was unsuitable for this study because the research question, objective, and context did not require such an approach.

Some of the qualitative research designs researchers use include pragmatic inquiry, ethnography, phenomenology, and narrative designs (Johnson & Christensen, 2020). I used a pragmatic inquiry design for this study. Researchers use pragmatic inquiry to answer research questions on *what, how,* or *why* (Ridder, 2020). Pragmatic inquiry enables researchers to determine the reasons for a phenomenon through interviews, participants' observations, and field notes (Taguchi, 2018). A natural environment allows participants to express their views and thoughts (Kelly & Cordeiro, 2020). Pragmatic inquiries are a method for eliciting data through introspection using semistructured interviews and thinking-aloud protocols to enable researchers to gain insight into participants' perceptions of their actions (Makin, 2021). The pragmatic inquiry design was appropriate for this study because it is an inductive approach that allowed me to identify, explore, and compare the effective strategies IT leaders of universities in Cameroon use to prevent or mitigate the costs of cyberattacks.

Researchers use the ethnographic method to understand how behaviors reflect a group's culture (Institutional Ethnography, 2020). The ethnographic design was not suitable for this study because the intent was not to study the behavior and culture of participants in this study. Researchers use a phenomenological design to understand lived experiences from a participant's perspective (Balikçi, 2022). The phenomenological design was unsuitable for this study because I did not plan to study the lived experiences of people or groups of individuals. I used the pragmatic inquiry for this study to identify and explore the strategies IT leaders of universities in Cameroon use to prevent or mitigate cyberattack costs.

Research Question

This study's overarching research question was "What strategies do IT leaders of universities in Cameroon use to effectively prevent or mitigate the costs of cyberattacks?"

Interview Questions

I used the interview questions below to address the research problem and answer the research question:

1. What strategies do you use to prevent cyberattacks in your institution?
2. How effective or successful are these strategies?

3. What challenges do you encounter implementing these Strategies?
4. What training do you have for your staff and students to fight against cyberattacks?
5. What policies and procedures have you adopted to address cyberattacks in your institution?
6. What additional information would you like to share regarding your strategies to prevent cyberattacks in your institution?
7. Is there anything else you would like to add?

Conceptual Framework

The conceptual framework of this study anchored on systems theory postulated by Von Bertalanffy. In 1968, Bertalaffy proposed the systems theory to describe the principle that the parts of a system can best be understood in the context of the relationships with each other and other systems rather than in isolation (Adams et al., 2014; Bertalanffy, 1968). The central tenet of the systems theory is that a complete system has interrelated parts instead of defining a system as individual parts. Systems theory is used in several fields, such as sciences, humanities, and technology (Adams et al., 2014; Bertalanffy, 1968). Systems theory has four main concepts: input, output, feedback, and environment (Hartnell et al., 2019). Systems theory is a combination of interactions used to expand an individual’s ability to recognize and comprehend systems while forecasting the performances and adjusting the systems to deliver the anticipated outcomes (Zhu, 2022).

Systems theory was suitable for this study because the theory is a holistic approach that views a complete information security system as contrary to viewing the parts as distinct entities. Understanding a whole system decreases the complexity of comprehending multiple parts of a system (Zhu, 2022). Integrating systems theory in this study assisted in exploring strategies to influence the system’s interconnections, feedback, and different performances. Recognizing interconnections and input in a system contributed to getting a better understanding of the system structure and allowed me to identify the organizational strength and weaknesses in designing and implementing these strategies (Zhu, 2022). System theory was also suitable for this study because it facilitated a proper understanding of the effective strategies IT university leaders could use to prevent or mitigate cyberattacks.

Operational Definitions

The following definitions of terms applied to this study.

Artificial intelligence: Developing computer systems that can perform tasks requiring human intelligence (Kizza, 2020).

Cyberattack: Invasion of computer or network devices by unauthorized individuals to cause harm to the system (Y. Li & Liu, 2021).

Cybersecurity: Cybersecurity refers to tools, policies, software, and processes in place to prevent or defend against malware and cyberattacks (Corallo et al., 2022).

Cybersecurity strategy: Cybersecurity strategies serve as a blueprint for building an effective, collaborative, enterprise-wide posture and defense against cyber threats (Bhamare et al., 2020*).*

Governance: The act of using regulations, internal policies, standards, and procedures (Tahir, 2018).

Assumptions, Limitations, and Delimitations

As with any qualitative study, assumptions, and limitations affected this study; mitigating these assumptions and constraints increased the validity of the research and prevented undue bias on my part.

Assumptions

This qualitative pragmatic inquiry was based on the following research assumptions. I assumed that the conceptual framework for the analysis was valid. I also assumed that participants spoke openly and honestly to ensure that information is protected. The respondents in this study were not subjected to social desirability bias. Given that respondents were asked about cyberattack prevention in their institutions, they experienced a need to answer more favorably because of control or peer pressure.

Limitations

The empirical results reported should be considered in light of some restrictions. The primary impediment to these results' generalization was that the sample size did not allow the transferability of findings to a general population in qualitative research. The research question and the conceptual framework created boundaries and limitations as the review explicitly focused on preventing cyberattacks within universities in Cameroon. I acted as the primary instrument for data collection and analysis.

This study's sample was limited to IT leaders of universities in Cameroon. This limitation was essential to control the scope, but other institutions or universities had different methods or concerns. Positivist researchers find pragmatic inquiry inadequate because they do not provide evidence of causal connections; using the pragmatic inquiry method precludes any external validity (Chang et al., 2020). In a qualitative study, given the reliance on participants' perceptions and opinions, subjectivity and imprecision exist that limits the possibility of confirming results (Creswell & Creswell, 2018).

Delimitations

Delimitations are the limits set by the researcher such that the study objective will be practically achievable (Theofanidis & Fountouki, 2018). First, I delimited this study to universities in Cameroon with an enrollment of over 5000 students. Second, I delimited the study to IT leaders who must have implemented effective strategies to prevent cyberattacks.

Significance of the Study

Contribution to Business Practice

It is estimated that business leaders would have to spend over $3.8 million to recover from a security breach. (Ho et al., 2023). Modern technology and innovations can keep business organizations safe and secure from cyberattacks (Meng et al., 2023). Business leaders need effective strategies to prevent the risk of cyberattacks. This study was significant because the findings could help cybersecurity managers in universities by providing strategies, processes, and practical techniques needed to prevent or mitigate the costs of cyberattacks. Universities use network systems and data security to conduct day-to-day activities (Meng et al., 2023). Data security breaches can result in significant data loss, identity theft, ineffective systems, and derivative costs. Implementing effective security strategies could lead to effective business practices by preventing and mitigating the effects of cyberattacks and should improve business performance. The findings of this study complement the existing literature focusing on typical Western organizations. Results showed how organizations in unique cultural, political, and legal systems prevent or mitigate cyber threats.

Implications for Social Change

This study's findings may contribute to a positive social change by giving university leaders confidence and the necessary procedures to safely secure students, staff's sensitive data, and improve the economy's health (Grewal et al., 2020). Furthermore, positive social change is implied through providing a safe and secure learning environment for universities to conduct daily business activities.

A Review of the Professional and Academic Literature

Introduction

Data breaches result in increased loss of sensitive data, identity theft, and business profitability (Trumbach et al., 2023). Emerging cyberattacks pose a significant threat to university institutions as universities increasingly rely on computer networks to conduct day-to-day business activities (Tayaksi et al., 2022). Cyberattack incidents increased by 125% through 2020, and increasing volumes of cyberattacks continued to threaten businesses and individuals in 2021 (Al-Ghamdi, 2021). The urgency to strengthen data security in university institutions increased as universities rely on technology and are the prime target for hackers (Alarifi, 2023). This qualitative pragmatic inquiry identified the strategies of IT leaders of universities in Cameroon to prevent or mitigate emerging cyberattacks. This study complements prior studies that focused on typical organizations in Western countries.

This literature review aims to present and discuss related issues and findings of previous studies relevant to this study. I recognized gaps in the past and current literature to validate the significance of this study. The literature analysis for this study began with a search of the university library databases: Google Scholar, SAGE journals, Digital Library, and books. I applied the Walden University Summons tool in all library searches; I used this tool to search multiple databases in a single request. The database searched in this literature review includes ProQuest, EBSCOhost, Science Direct, and JSTOR. I used the Summons tool scholarly and peer-reviewed options to refine the search to peer-review and academic journals and limited the search results to studies published within the last 7 years. I used these databases to explore both current and seminal works regarding cybersecurity management.

The keywords used for searching the literature for this study are *systems theory, cyberattack, cyber impact, information security risk, privacy and protection, Chief information security officer, cybersecurity, systems theory, artificial intelligence, and strategies for data security*. I conducted 60 searches using the Google Scholar search engine with the exact keywords and combinations. This additional search allowed me to identify any literature that may have been left out in the previously searched databases. I searched the Sage Knowledge and Sage Research Methods databases to develop this study's research design and understand less standard research methodologies, models, and related terms discovered in the existing literature under review. I retrieved more than 1,000 articles in the queries from all databases. After reviewing the abstracts and delving into related articles to determine their relevance, I found 168 articles relevant to this study, and the articles were downloaded for inclusion in the literature review. According to Walden University’s DBA program, 85% of the referenced sources have been published within the past five years, enhancing the relevance and currency of the academic argument (Walden University, 2023). I used various sources in my literature review, most of which are peer-reviewed and published between 2019 and 2023. As a part of the literature review, academic books, dissertations, and data articles were also reviewed (see Table 1).

Table 1

Literature Review Content

Category	Result
Total number of references	168
Number of references within five years	148
Number of peer-reviewed references	160
Percentages of references with five years	88.10%
Percentages of peer-reviewed references	95.2%

The literature review of this study began with searching presenting sources, databases, and keywords used to search peer-reviewed and scholarly journals for studies published within the last 5 years. The specific sections in the review of literature are the following: systems theory, the concept of cybersecurity, social media, and cybersecurity risks on universities, emerging trends in cybersecurity, effects of cyberattacks on the universities, and IT strategies for preventing and mitigating cyberattacks. The last section is a summary of the literature review and transition to the next section.

System Theory

The theory that grounds this study includes the system theory postulated by Von

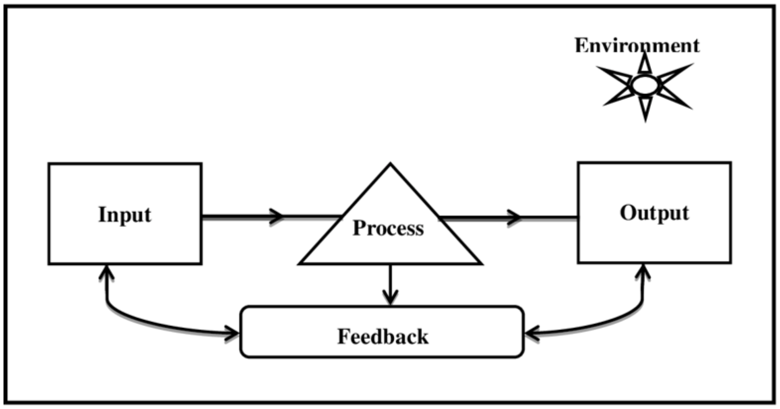
Bertalanffy in 1968. Systems theory describes the principle that the parts of a system can best be understood in the context of the relationships with each other and other systems rather than in isolation (Adams et al., 2014; Bertalanffy, 1968). Systems theory was first developed to comprehend organisms in the field of biology but was later extended beyond the field of biology to study several areas (Klier et al., 2022). Business leaders use systems theory to explore people's actions in diverse fields, such as sciences, humanities, and technology (Adams et al., 2014; Bertalanffy, 1968).

The central tenet of the systems theory is that a complete system has interrelated parts instead of defining a system as individual parts. According to Bertalanffy (1968), systems are open or closed systems thinking. In available systems, the inputs interact with the environment; in secure systems, there is no interaction between the information and the environment (Klier et al., 2022). Organizational leaders choose open systems over closed systems because open systems facilitate interaction with other business operations and subsystems. The subsystems intermingle with the environment. Organizations are considered open systems, hence interacting with their environment. The organization's interaction with its environment helps to identify which component of the system is not working at total capacity, thus affecting the overall productivity or functionality of the system (Thimm, 2022). For instance, open systems allow university leaders to interact with shareholders, students, and faculties in business organizations such as universities. Closed systems are autonomous, hence not requiring interaction with the environment to function (Klier et al., 2022).

Systems theory has four main concepts: input, output, feedback, and environment (see Figure 1). The input and output components are carriers of data that enable system openness to determine the quantity and frequency of information transported through the System and feedback are output information loaded into the system as input (Adams et al., 2014). Business leaders apply feedback to comprehend the performance or efficiency of information in a system (Klier et al., 2022). Using the information in a system can result in positive or negative changes within a system. Positive feedback is experienced when the system functions appropriately without interruption, while negative feedback is when the data path is disrupted (Zhu, 2022). Systems theory is a combination of interactions used to expand an individual's ability to recognize and comprehend systems while forecasting the performances and adjusting the systems to deliver the anticipated outcomes (Zhu, 2022).

Figure 1

System Theory Central Tenets



Note. The system theory central tenets. Adapted from "Systems Theory as the Foundation for Understanding Systems" by K. M. Adams, P. T., Hester, J. M. Bradley, T. J. Meyers, and C. B. Keating, 2014, *Systems Engineering*, *17*(1), p.

134.1https://doi.org/10.1002/sys.21255

When IT leaders view the organization as a complex system, some vital concepts include open systems, synergy, and subsystems. Open systems interrelate with their environment to determine their best fit (Klier et al., 2022). Most business institutions are regarded as open systems and interact with their environment. Thus, systems theory is used to examines complex systems such as hospitals, educational institutions, and companies (Vanderstraeten, 2019). Based on an extensive literature review, university institutions can be viewed as open systems through the lens of systems theory. The interaction with the environment helps to identify which component of the system is not working at full capacity, thus affecting the overall productivity or functionality of the system.

Most organizations also comprise subsystems (Klier et al., 2022). Through the lens of systems theory, the organization is considered a purposeful system of interconnected subsystems working together to accomplish the organizational goals, and any modification in one subsystem affects the organization (Klier et al., 2022). Synergy is also another crucial element of complex systems; the organizational subsystems achieve more when they work harmoniously (Hartnell et al., 2019). Applying a systems theory concept can enable the researcher to comprehend the root cause of a problem and find possible solutions to make the system more efficient and reliable. According to systems theory, nothing can be understood in separation; instead, it should be viewed as a component of a more extensive system (von Bertalanffy, 1968).

As business leaders continue to welcome technological innovations, organizations must endorse these new technological advancements, and organizational parts must work as one (Han et al., 2023). To realize this objective, IT leaders must implement strategies to meet organizational goals and protect corporate data from cyberattacks (Han et al., 2023). A systemic approach to data security management is centered on impending the systems is an integrated data security system characterized by the accomplishment of a stable state through the involvement of all the system components (Y. Connolly & Wall, 2019). Any interruption in the organizational data system might threaten the organization's future. IT leaders should consider this to guarantee the system's or organization's survival (Mierzwiak et al., 2019). Thus, systems theory provides a substantial baseline for efficiently managing cybersecurity (Zenker & Kock, 2020). Exploring the effective strategies used by IT leaders to prevent cyberattacks could serve as best practices, boost customer confidence, and stimulate economic growth (Dias et al., 2022).

Systems theory is suitable for this study because the idea is a holistic approach that views a complete information security system as contrary to viewing the parts as distinct entities (Chatterjee, 2021). Understanding a whole system decreases the complexity of comprehending multiple parts of a system (Yun et al., 2019). Integrating systems theory in this study assisted in exploring strategies to influence the system's interconnections, feedback, and different performances. Recognizing interconnections and input in a system will contribute to getting a better understanding of the system structure and allow me to identify the organizational strength and weaknesses in designing and implementing these strategies (Zhu, 2022). Further, system theory is suitable for this study because it could facilitate a proper understanding of the effective strategies IT university leaders could use to prevent or mitigate emerging cyberattacks.

Supporting and Contrasting Theories

Following the nature of this study, systems theory was selected as the conceptual framework to aid in comprehending the phenomena and explore the strategies university IT leaders apply to prevent or mitigate emerging cyberattacks. This section presents theories that support or contrast systems theory as the selected theory for this study. There are several theories that a researcher can choose for the study. However, the researcher must determine which theory will best address the problem statement and answer the research question before selecting it. There are a series of cybersecurity theories, such as the theory of information warfare and the theory of protection motivation (Dias et al., 2022).

Theory of Information Warfare

The information warfare theory is newly developed compared to systems theory. The origin of the information warfare theory is associated with Sun Tzn, following massive improvements in communication and technology (Werder & Maedche, 2018). The enormous progress in communication and technology generated strategic consequences that impacted the government, the military, and the general public (Monov & Karev, 2018). Information warfare is about gathering, providing, and denying information to improve decision-making while damaging the enemy (Monov & Karev, 2018). Today, information warfare is given different names representing several dimensions with other purposes. In modern technologies, the information warfare theory consists of modern means of messaging, indicating a certain level of restricted war carrying a low level of escalation while offering chances for geopolitical improvement goals at a slight cost (Libicki, 2020). Information warfare is a transnational threat, mainly affecting national security, penetrating national borders, and weakening stability (Libicki, 2020). The theory of information warfare is more about encouragement to leaders, the general public, and control over actions and decision-making (Monov & Karev, 2018). Therefore, the information warfare theory is more applicable when national security circumstances affect the government and the defense force and was not suitable for this study.

High-Reliability Theory

Another theory that supports system theory is the high-reliability theory developed in 1987 to comprehend why reliable businesses are hierarchically low in errors or failures (Scott et al., 2023). One prominent feature of highly reliable organizations is their determination not to be content with the status quo of their current level of safety (Scott et al., 2023).), unlike systems theory, which inspires scholars to consider organizations and their environment as one entity rather than as individual entities. According to R. M. Rice (2021), the highly reliable theory involves studying organizations capable of evading errors while providing adequate competencies under an extensive environmental situation. The systems theory and highly reliable theory consist of complex systems and how the environment affects the system’s general performance. However, according to Scott et al. (2023), high-reliability theory focuses more on nuclear plants and air travel organizations that manage operations with disastrous consequences, while systems theory, on the other hand, applies to several organizations such as universities.

Grey System Theory

Grey systems theory is another theory that I considered but was not selected because it did not satisfy the need of this study. Researchers could employ grey systems theory in contrast to systems theory. Grey systems theory was developed in 1982 by Julong Deng to bridge the gap between natural and social sciences (Deng, 1982). According to Hofkirchner (2019), grey systems theory is said to have knowns and unknowns. Hence any business problem is studied with a small sample or incorrect data leading to wrong assumptions or luring conclusions based on limited information. In contrast to grey system theory, systems theory will aid the researcher in recognizing the problem, creating patterns, and establishing relationships (Dailey et al., 2023). All the elements associated with this study's business problem are identified, so systems theory is selected as the conceptual framework to guide this study.

Finally, systems theory is chosen as the conceptual framework to ground this study because I can apply it to universities as it satisfies the conditions of being classified as an open system. Systems theory encourages a holistic approach when investigating a business problem which will guide the researcher in this study to explore the strategies that IT leaders use to prevent or mitigate emerging cyberattacks in universities. Furthermore, applying systems theory in this study, universities can be viewed as a purposeful system with interconnected subsystems working harmoniously to accomplish a mutual goal. The remainder of this section will cover the main themes discovered during the literature review for this study.

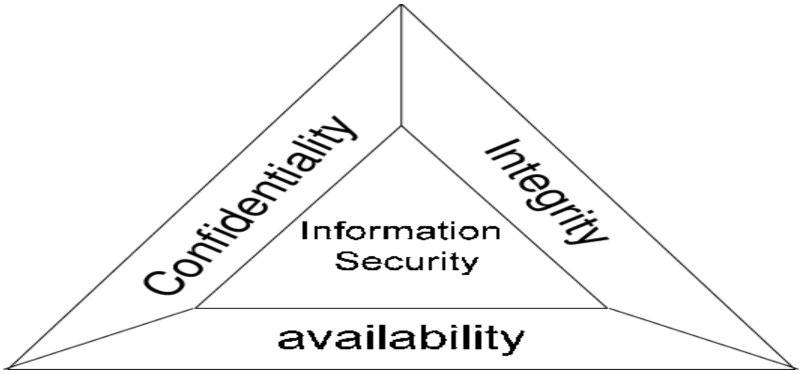
Concept of Cybersecurity

Internet usage increased significantly during this pandemic, with sizable interconnected networks facing multiple threats (Barik et al., 2022). As a result, there are numerous security threats in cyberspace. According to Barik et al. (2022), cyberattacks are increasing rapidly due to advanced digital technologies used by hackers, and cybercriminals are conducting cyberattacks, making cyber security a rapidly growing field. The National Institute of Standards and Technology (NIST) defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks (Arpaci & Sevinc, 2022). User and organization assets comprise connected services, applications, devices, systems, and stored or transmitted data in cyberspace (Coenraad et al., 2020).

Security leaders or professionals aim to ensure business continuity by preventing and mitigating the impact of security incidents that threaten organization information assets and protecting information and its critical elements, including systems and hardware that store and transmit (Tsaregorodtsev et al., 2019). The organization’s three primary cybersecurity goals are known as CIA-triad: confidentiality, integrity, and availability (see figure 2). The CIA triad guides IT leaders to understand and address related security problems (Tsaregorodtsev et al., 2019). Confidentiality is the ability to protect information from unauthorized disclosure; Integrity is the ability to ensure the accuracy and competence of information, and availability is the ability to ensure that information is readily accessible to authorized users when needed (Miloslavskaya et al., 2018).

Figure 2

The CIA Triad



Note. The CIA triad. Adapted from “Biometric system for protecting information and improving service delivery: The case of a developing country’s social security and pension organization” by Owusu-Oware and Effah, 2022, *Information Development*, *0*(0), p. 4. https://doi.org/10.1177/02666669221085709

Cybersecurity, from a theoretical perspective, comprises technical controls and leadership. Apart from technology, the fundamental direction of the cybersecurity approach involves governance and management as primary aspect of security (Tsaregorodtsev et al., 2019). According to Whitman and Mattord (2022), the fundamental element of cybersecurity is to ensure the CIA (confidentiality, integrity, and availability) of information, referred to as the CIA security model (Whitman & Mattord, 2022). Whitson advocated that organizations attain security through risk analysis, security policies, security training, and awareness, as well as developing a plan for disaster avoidance and recovery (Whitman & Mattord, 2022). Despite the CIA security model’s appearance and other security standards and frameworks, there is no common ground for deploying a standard approach to cybersecurity management. Organizations are trapped by the scientific CIA opinion on one hand and by the actual incorporation within corporate governance. Security policy, compliance, and awareness are the three cornerstones of capable cybersecurity architecture (Xiong & Lagerström, 2019).

Security Policy

Security policy is a cornerstone for capable cybersecurity architecture, yet it has shortcomings, such as developing a good understanding of security policy and implementing it (Lena et al., 2019). Security policies are noted in the literature as a primary control organization can implement to protect their data (Shields et al., 2020). Besides the investment in information security technologies, such as antivirus, firewalls, backup systems, and cybersecurity awareness, training and education programs are essential for organizations to implement security policies (Shields et al., 2020). According to Peterson et al. (2022), security policy is a set of laws, rules, and practices regulating how an organization protects and distributes resources to achieve specific security objectives.

The security policy determines the organizational direction and users' practical actions (Shields et al., 2020). The main objective of security policy is to assess information resource users' rights and responsibilities (Peterson et al., 2022). Security policy is an organization's baseline for implementing cybersecurity (Klier et al., 2022). According to Klier et al. (2022), a positive correlation exists between effective security policy and cybersecurity implementation. According to Peterson et al. (2022), security policy is the primary enabler of processes within the organization and the continuous operation of information systems. The literature strongly advocates for the importance of security policy; inadequate or insufficient implementation can weaken the information security process and render information security useless (Peterson et al., 2022)

Security Compliance

Engaging in security awareness activities helps foster a culture of compliance toward information security in the organization. Security incidents such as the Sony Pictures breach 2014 indicate that confidential information is at risk (Pacella, 2016). According to Yun et al. (2019). researchers consider human behaviors in technology to enhance information security compliance. Lee and Hong (2020) supported this view in their study on physicians' diligence in protecting confidential patient information. They found that physicians would put data at risk if protecting them impedes their job functions despite the growing importance of information security (Lee & Hong, 2020).They further found that those with access to confidential information are not driven to protect them correctly when they believe more critical work needs to be done. Lee and Hong (2020) provided a motive to consider user behavior to secure confidential data through information security compliance. Reeves et al. (2021) supported Bicaku et al. (2020) motive and further recommended a better understanding of individual behavior in securing confidential information. Lee and Hong (2020) findings are significant because Lee and Hong (2020) assume that the user's practice diligently complies with information security policies; however, these assumptions of compliance may be incorrect, and Scholars and practitioners should not accept that security policies are consistently followed (Reeves et al., 2021).

Bicaku et al. (2020) used the protection motivation theory to develop a fear appeal rhetorical framework to judge information security policies' effectiveness when individual employees are affected through personal relevance. The study found that particular significance substantially positively influences compliance using the model. Bicaku et al. (2020) surveyed the Finnish city government as the population, limiting the ability to globalize the study results. Bicaku et al. (2020) study provides insight into human behavior concerning personal relevance influencing compliance with information security policies.

Other studies have also observed compliance performance and information security. Fawehinmi et al. (2020) attempted to determine the human behavioral factors that lead to using and complying with information security systems. The authors extended the technology acceptance model (TAM), which looks at technology's perceived ease of use and usefulness (Mlekus et al., 2020). Mlekus et al. added social impact, perceived cost, technology utility, individual innovation, and computer self-efficacy to TAM. The authors found that social influence factors positively affect an individual's intent to use information security mechanisms. The study had significant results, but the population was limited to China. Cultural differences may impact compliance because the research relates to human behavior (Mlekus et al., 2020)

The literature views cybersecurity compliance through expected avenues. Kour et al. (2020) conducted an action research study on user training effectiveness to improve information security policy compliance. Kour et al. (2020) developed a training program based on the universal constructive instructional theory and the elaboration likelihood model. Kour et al. (2020) research aimed to test the effectiveness of user training developed using theory-driven methods. Empirical research in developing information security training is a constructive step in the field; however, the findings suggested that social influences are a large part of motivating compliance behavior. Fawehinmi et al. (2020) included understanding the social consequences of compliance behavior. Training may positively affect compliance behavior, but it is not the only factor. To enhance security compliance, the organization must create a compliance culture (Fawehinmi et al., 2020). The culture of compliance is achieved by implementing an effective cybersecurity program that deals with all organizational levels, conveys information security, and promotes cybersecurity awareness (Bicaku et al., 2020).

Cybersecurity Awareness

Security awareness is an initiative activity in an organization that aims to ensure that both management and the end-users are aware and dedicated to security, risk reduction, security policies, and standards (Rahim et al., 2019). Cybersecurity awareness is essential because information security techniques concerning the information system can be misused or poorly implemented, thereby making security guidelines ineffective (Xiong & Lagerström, 2019). The effectiveness of security awareness relies on the willingness of individuals to receive it. Awareness activities cannot be productive without a genuine interest in information security (Whyte, 2022).

Although security awareness is a crucial function in the organization, security awareness is underfunded and implemented in an ad hoc process. Security awareness is unstructured in many organizations (Back & Guerette, 2021). To promote security awareness, organizations must create a security culture by implementing security techniques that aim at all levels: employees, top management, and end-users (Back & Guerette, 2021). Prior studies have considered cybersecurity security awareness an essential enhancement factor for cyberattack prevention control. Surveys show that despite the significant role of security awareness in cybersecurity management, less than 30% of organizations have security awareness schemes (Aydin, 2021). Little attention is given to security awareness, and most awareness activities are neglected in organizations despite the direct relationship between security awareness and compliance (Rahim et al., 2019).

The ability to connect securely to virtual networks is the case within universities. Students are increasingly learning in digital formats; faculty, staff, and visitors continually access and share information online, and more infrastructure and facility functions are managed online (Soomro et al., 2020). To maintain a collaborative culture, universities must effectively secure the network, physical, cloud environment, and Internet of Things (Soomro et al., 2020). There are four significant types of cybersecurity: network security, physical security, cloud security, and Internet of Things (IoT) security.

Network Security

Network security is critical to the day-to-day IT operations of nearly every organization. Network security protects organizational data from unauthorized entry through the computer network (Tao et al., 2020). Network security consists of software, hardware, and technology working harmoniously to protect corporate data from several threats. According to ThiBac and Minh (2022), network security serves as a wall between the network and malicious activities, and organizations such as universities must protect the network to ensure the continuous delivery of services to meet the demands of stakeholders (Bada & Nurse, 2019). Examples of network security include a firewall that acts like a barricade between an internal trusted network and external Internet, email security that helps to stop any incoming attack, preventing loss of sensitive data, and an antivirus that allows scanning Malware upon entry (J. Sun, 2022).

Physical Security

A key component of cybersecurity is physical security, as loss of hardware, espionage, and data theft can occur due to physical security breaches (Chandna & Tiwari, 2023). There will be a great deal of variation between universities concerning the level of physical security due to location and climate. However, we did find some generic discussions about campus physical vulnerabilities: Universities generally practice very little physical security due to their open and inclusive academic culture. Cameroon University campuses lack physical security as there are no physical access controls. If they do, Tao et al. (2020) reported, it is impossible to enforce access control or determine who is responsible for a security incident. Typical university incidents include theft, loss, and damage to portable/stationary devices. In all these cases, a weak physical access control system and security for physical equipment contribute to the threat event (Tao et al., 2020).

Cloud Security

According to Mthunzi et al. (2020), many organizations, including universities, face the risk of cloud security. To better store and share information, many universities have adopted cloud computing to create a virtual repository for data storage and an invisible channel through which information is shared (Vinoth et al., 2022). Cloud computing makes collaboration easy in the learning environment. However, cloud computing puts universities at risk for cyberattacks, especially when PII, operational data, financial aid data, and other sensitive information are stored on third-party servers accessible over the Internet (Khoda Parast et al., 2022). Cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and cloud computing's associated infrastructure (Alraja et al., 2023). Cloud security primarily emphasizes the vulnerabilities of Internet services and shared environments (Mohammad & Pradhan, 2021). It protects the application and Infrastructure security from cloud-connected components. Universities are recommended to implement and perform a routine revision of their cloud computing policies to protect data (Lopez Garcia et al., 2020)

IoT Security

Another aspect of cybersecurity is the Internet of Things. This is a network of all physical devices connected to the Internet, such as appliances in the home (Mthunzi et al., 2020). There are many benefits to using the Internet of Things, but the organization also faces several risks (Ravikumar et al., 2022). For example, a hacker could access organizational IoT devices and compromise sensitive data, including financial records (Kaur et al., 2023)). Organizations must take the necessary steps to secure IoT devices to protect themselves against these risks. A few strategies to consider are using strong passwords, updating devices regularly, and installing apps from trusted sources (Kaur et al., 2023). In social media channels over the Internet, cybercriminals can exploit internal information or employee contacts to perform phishing attacks and identity theft (Aydos et al., 2019).

Social Media and Cybersecurity Risks on Universities

Generally, a social network is a group of individuals or organizations with at least one connection (Whyte, 2022). Businesses use social media to boost brand recognition and connect with consumers. Social media use has become so popular that companies are unaware of the numerous cyber risks that they pose (Ali & Mohd Zaharon, 2024). According to Ali and Mohd Zaharon (2024), more than 59% of the global population uses social media platforms at least once daily, or almost 4.8 billion people. People and businesses are increasingly exposed to cyber threats due to social media platforms, which help users keep in touch with friends, connect with customers, and promote businesses (Whyte, 2022). A business's risk of social engineering attacks increases when using social networks, even though social media is an indispensable marketing tool for modern companies (Neumann & Rhodes, 2023). Cybercriminals can exploit social media channels to perform phishing attacks, credential thefts, data thefts, and other scams by posting internal information or employee contacts (Neumann & Rhodes, 2023).

Regarding social media usage, university students, such as Facebook, Twitter, Snapchat, and YouTube, are the most active users as reported by Neumann and Rhodes (2023). As a result, Malware and other viruses, such as wildfire, will be hosted and spread through this mechanism by using social media sites (White & Forrester-Jones, 2020). There is no way to block access to social media permanently in a university setting. Identifying infected devices as soon as possible is essential, and the cyber team should maintain data and network security.

The demands for cybersecurity in universities will continue to increase. Serious data breaches have occurred already and are likely to happen again without effective strategies implementation (Greyson et al., 2023). Universities and other academic institutions have become lucrative targets for cyberattacks and have suffered multiple high-impact incidents (Adebayo & Ninggal, 2022). University institutions manage large amounts of valuable research and sensitive personal data, which makes them an attractive target for cyber-criminals, espionage, and hacktivists (Adebayo & Ninggal, 2022). The threat landscape consists of everything from opportunists seeking financial gain to heavily funded state-sponsored actors who intend to steal trade secrets (Primack et al., 2019).

Furthermore, the free flow of the workforce and annual rotations of new students, guest, and employees also adds to the universities' information security challenges (Primack et al., 2019). Even though academic institutions face substantial cyber risk at their institutions, the initiative to implement cybersecurity measures varies, and the cost of recovering from a cyberattack on universities is similar to that of other organizations (White & Forrester-Jones, 2020). Cyberattack plight is not without severe consequences; students' data can be compromised, research information exposed, and even government data can be stolen. Furthermore, universities can close down for days due to attacks such as Distributed Denial of Service (DDoS) and ransomware attacks (Primack et al., 2019).

Long-term reputational damage can have a profound impact on enrollment levels. A fundamental characteristic of the academic community is that it is a place to share knowledge. However, there are some critical vulnerabilities when ensuring security (Whyte, 2022).

Consequently, almost three-quarters of the attacks launched against colleges and universities have been successful. The number of successful attacks in the business sector was 68% compared to 75% in the educational sector (Leal & Musgrave, 2023). It has become increasingly clear that university students and staff are at risk of various threats (Arpaci & Sevinc, 2022). The educational industry faces similar vulnerability as other organizations but is often deeper in the academic sector. The security managers within the institutions are responsible for protecting, securing, and storing institutional information. This information includes financial aid administration containing student and family personally identifiable information (PII), research information, intellectual properties, online learning portals, and other operational data within the institution (Arpaci & Sevinc, 2022). This information puts the institution at high risk for the cyber threat that aims at obtaining sensitive information. According to Leal and Musgrave (2023), organizational leaders such as university administrators and managers are recommended to work closely with the cybersecurity team to prevent, protect, mitigate, respond to, and recover from cyber threats. The most commonly used cyberattack methods on university systems are Phishing, Denial of Service (DOS), Malware, and Ransom.

Phishing

In cybersecurity, studies show that phishing is the most common threat affecting everyday internet users. The phishing attack attempts to gain sensitive information effectuated through email by malicious individuals or groups (Lee & Hong, 2020). Phishing victims are usually targeted through fraudulent emails that hyperlink to fake websites through which users are urged to release sensitive information like home addresses, usernames, and passwords (Tornblad et al., 2021). Criminals use so-called social engineers to trick users, infecting computers with viruses, stealing their money from cards or their identity, taking their data, and even some digital documents related to studies or research (Verma & Shri, 2022). In recent years, phishing attacks have become an increasingly prevalent problem in universities. As a result, Cameroon universities are exposed to much risk, even more than institutions in other parts of the world. To mitigate the risk of phishing attacks, universities should employ cybersecurity training to enhance individual preparedness.

Denial-of-service (DOS)

One of the most common types of cyberattacks is a denial-of-service attack, also known as a DDoS attack (Zhao et al., 2023). Universities face several dangerous cyber threats. As a result of a successful DOS attack, there can be significant financial implications. It has been reported in security surveys that DDOS attacks are estimated to cost between $ 20,000 and $ 40,000 per hour on average in the case of a DDOS attack (Aydos et al., 2019). The Denial-of-Service attack is a cyberattack that affects one computer or several computers connected simultaneously and affects the ability of legitimate users to access resources by reducing, restricting, or preventing access to those resources, such as email, learning accounts, and websites (Zhao et al., 2023). In a DDOS attack, an attacker will create a flood of traffic or service demands on the victim's system to overwhelm the system (Bu et al., 2023). University cybersecurity departments should deploy antivirus software, firewalls, and policies to mitigate denial-of-service attacks.

Malware

Malware is another type of attack vector for universities. This attack occurs when unauthorized or unrequested software is installed on individual computers or institutional servers, limiting access or courses the system to crash (Verma & Shri, 2022)). Feng and Wang (2019) state that Malware may include ransomware, viruses, worms, and adware. Malware threats often steal information to commit fraud. Universities are hosts of bring-your-own-everything (BYOE) environments, and at such, students, faculty, staff, and visitors bring everything, such as smartphones, tablets, laptops, desktops, and other navigation devices, to meet educational and social needs (Chigada & Daniels, 2021). BYOE enhances information sharing, digital learning, and how individuals can access university networks. Some BYOE devices are unsecured, rendering university networks and systems vulnerable to attacks (Chigada & Daniels, 2021). Monitoring and routine risk assessment are recommended as university cybersecurity management efforts.

Ransom Attacks

An attack known as ransomware is malicious software designed to encrypt a system to prevent its operation until the money is paid (Niki et al., 2022). Even though ransom attacks usually target individuals, it's only a matter of time before groups become victims (J. Davis & Wilner, 2022). This is standard practice at Cameroon University. This attack mainly targets the devices of all those who connect to their networks, students, staff, and visitors (J. Davis & Wilner, 2022). A lock screen is typical in all encryption programs, screen lockers, and other types of digital currency. These screens encourage victims to buy cryptocurrencies, such as Bitcoin, to pay ransom (Cojocariu et al., 2020). The decryption key is given to the victim once the ransom has been paid, and the victim may then attempt to decrypt the file decrypt files (Cojocariu et al., 2020). However, multiple sources report varying success rates with decryption, so it is not a guaranteed process. Sometimes, the victim never receives the keys after paying the ransom, and malicious software is installed on a computer during an attack (Cojocariu et al., 2020). Often, ransomware victims who pay the ransom get their information retrieved by future attacks until the victim pays another ransom (Y. Connolly & Wall, 2019). In recent years, there has been a significant increase in cyberattacks of this type in universities. According to Datta and Acton (2022), cyberattacks become less likely to occur as cybersecurity processes become more automated by reducing the time needed to detect and respond to threats and improving detection accuracy.

Emerging Trends in Cybersecurity

Companies across many industries are being victimized by cybercrime every day. As a result, it has emerged as one of the greatest threats facing companies today (Trumbach et al., 2023). According to Arpaci and Sevinc (2022), cyberattacks have increased in recent years, with the number of attacks increasing rapidly worldwide and business costs growing. Cybercriminals are becoming more sophisticated and innovative each year, and the threat will only grow as they become more sophisticated and intelligent. (Arpaci & Sevinc, 2022). Data breaches can be prevented by using traditional security methods, but these methods are not adequate in the case of cyberattacks. Cybercriminals have developed new hacking techniques and robust tools to exploit, attack, and breach data (Trumbach et al., 2023). Artificial Intelligence (AI) technologies are introduced to cyberspace to create intelligent models that protect systems from attack (Chandna & Tiwari, 2023). Rapid technological development has led to artificial intelligence's development in cyber security through its ability to analyze data and make decisions (Chandna & Tiwari, 2023).

According to Bada and Nurse (2019), universities are facing a massive cyberattack surface, which continues to grow alarmingly. An organization's cybersecurity posture requires more than just human intervention to be analyzed and improved (Carlton et al., 2019). Artificial intelligence and machine learning to detect cyber threats have become increasingly crucial to cybersecurity because they can quickly analyze millions of data sets and track down a wide range of threats — from malware threats to shady behavior that could lead to phishing attacks (Chandna & Tiwari, 2023). This technology continuously learns and improves based on experience and current data, thus identifying new attacks that may occur in the future (Chandna & Tiwari, 2023). There are many ways in which artificial intelligence can be used to improve cybersecurity. As cybercrime trends evolve, artificial intelligence and machine learning can improve the ability to detect threats, respond more effectively, and keep up with cyber criminals (Dasgupta et al., 2022).

The Identification of New Threats

Artificial intelligence can be used to detect cyber threats, as well as potentially malicious activities on the Internet (Slepian & Jacoby-Senghor, 2021). The sheer volume of new Malware generated every week is challenging for traditional software systems to keep up with, so this is an area where Artificial Intelligence can make a difference (Dasgupta et al., 2022). The AI system is trained by sophisticated algorithms, running pattern recognition and identifying even the minutest behaviors of malware or ransomware attacks before it infects the system, so they can be detected before it gets into the system (Dasgupta et al., 2022). In addition to predicting cyber threats, artificial intelligence allows natural language processing to curate data due to scraping articles, news, and studies on cyber security (Dasgupta et al., 2022). The results of this analysis identify new anomalies, cyberattacks, and preventive strategies. A cybersecurity system based on artificial intelligence can provide an in-depth understanding of global and industry-specific threats, which can help you make essential decisions based on what is most likely to be used against organization systems, not just what could be used to attack organization systems (Dasgupta et al., 2022).

Defending Against Internet Bots

Internet traffic today is dominated by robots, which can pose a threat. Internet bots or robots can be dangerous for various reasons, from account takeovers using stolen credentials to bogus account creations and data theft (Dasgupta et al., 2022). Manual responses alone will not be able to counter automated threats. Universities can use the integration of artificial intelligence or artificial intelligence technologies to optimize website traffic and distinguish between good bots, such as search engine crawlers, and bad bots, like humans (Mohammad & Pradhan, 2021). The deployment of artificial intelligence allows cyber teams to analyze massive amounts of data and adapt cybersecurity strategies to a rapidly changing environment (Kenny et al., 2022).

Breach Risk Prediction

Organizations using artificial intelligence can create an accurate and detailed inventory of all of their IT assets that give them a comprehensive analysis of all devices, users, and applications allowed access to particular systems at various levels based on their permissions (Kenny et al., 2022). As a result of a coordinated analysis of asset inventory and threat exposure, AI-based methods can forecast how and where a business will most likely be compromised to plan appropriately and allocate resources to areas most likely compromised (Mohammad & Pradhan, 2021). The insights gained from AI-based analysis enable the organization to improve cyber resilience by modifying cybersecurity controls and processes (Mohammad & Pradhan, 2021).

Better Endpoint Protection

An increasing number of devices are used to work remotely, and artificial intelligence is essential in securing all these devices (Dasgupta et al., 2022). Antivirus solutions and VPNs can protect organizations from remote malware and ransomware attacks. However, these services tend to work by relying on signatures. It is, therefore, essential to stay up-to-date with signature definitions to stay protected from the latest threats (Dasgupta et al., 2022). When virus definitions lag due to insufficient updates or a lack of awareness from software retailers, this can lead to a security concern. For this reason, a signature protection system may be unable to protect against a new malware attack (Dasgupta et al., 2022).

In contrast to the traditional method, AI-driven endpoint protection adopts a different approach, which involves establishing a baseline of behavior for the endpoint through repeated training to prevent future attacks (Kenny et al., 2022). The AI can flag unusual events and take appropriate action such as sending a notification to a technician or returning the system to a safe state after a ransomware attack (Kenny et al., 2022). The advantage of this is that it provides proactive protection against threats rather than waiting for updates to existing signatures.

Cybersecurity experts can use artificial intelligence (AI) to strengthen cybersecurity best practices and lessen the attack surface instead of constantly on the lookout for malicious activity that might occur (Mohammad & Pradhan, 2021). As IT security teams strive to improve their efficiency with AI, it is becoming a must-have technology, according to Mohammad and Pradhan (2021). A human being cannot adequately secure an enterprise-level attack surface, and artificial intelligence provides the analysis and threat identification that security professionals need to minimize breach risk and enhance security posture (J. Sun, 2022). Furthermore, AI can lead to the discovery and prioritization of risks, effective event response, and early detection of malware threats (J. Sun, 2022). Despite AI’s potential downsides, artificial intelligence contributes to advancing cybersecurity and assists organizations in strengthening their security posture (Kenny et al., 2022).

Effects of Cyberattacks on Universities

Cyberattacks continue to increase across the globe, and educational institutions aren’t immune to the dangers of cyberattacks, which are on the rise (Prasad & Chandra, 2023). Cyberattacks have become one of the most prevalent university threats in recent decades, with devastating consequences. In today’s digital world, university store increasingly personally identifiable information (PII) about students, teachers, and staff. Universities are among the prime targets for cyberattacks because they keep a lot of PII about students, including student grades, financial aid, social security numbers, medical records, and research data. In the face of cyberattacks, universities can face severe and sometimes even life-threatening consequences, some of which may extend beyond the immediate effects.

Effects on Learning

In the wake of a cyberattack, universities can be forced to shut down, disrupting classes, obstructing students’ access to education, and ultimately hindering academic performance (Shaikh & Siponen, 2023). University closures can have much more severe consequences in districts where students depend on free lunch programs for a portion of their meals than just lower grades in the classroom (Prasad & Chandra, 2023).

Effect on University Reputation

As a result of cyberattacks, trust between students, families, teachers, and administrators can be compromised (Shaikh & Siponen, 2023). There is a high probability that an attack will draw negative media attention to the university, even if that attack is not intentional, which can be challenging to recover from for a university

(Soomro et al., 2020). In addition to the damage to a university's reputation, such an incident can result in difficulty in attracting and retaining staff and students due to the damage caused.

Effect of Compromised Information

The consequences may be severe if an attacker can access sensitive information through a cyberattack. As long as attackers have access to personal information, they can commit crimes such as identity theft which can have long-term consequences for the victim's credit history (Soomro et al., 2020). Cyberattacks against universities can result in unauthorized charges and funds being stolen from the district due to financial fraud (Shaikh & Siponen, 2023). Unfortunately, cyberbullying can also occur due to these security breaches because obtaining personal or medical information can lead to the intimidation or harassment of individuals (Shaikh & Siponen, 2023).

IT Strategies for Preventing and Mitigating Cyberattack Cost

Technology advancements and a dynamic environment create a complex landscape with the advent of Web 2.0 and its associated territory. Coping with cybersecurity-related challenges has become increasingly challenging (Cathcart, 2019). A study by Mansfield-Devine (2018) confirms that digital security threats are becoming more intense and complex daily. As the threat landscape evolves, more dynamic measures are required to curb cyberattack incidents (Feng & Wang, 2019). Over the past few years, a rise in cyberattacks has seen compensated investments to mitigate this threat. According to Kaur et al. (2023), a Gartner survey conducted in 2015 estimated $7.1 billion in information security expenses in 2014. In 2015, cybersecurity investments totaled $76.9 billion, confirming the trend (Kaur et al., 2023). Protecting sensitive information is becoming increasingly crucial for businesses.

Furthermore, Home Depot responded to the Target data breach by investing a massive amount of money in reforming security infrastructure to upgrade cash flow with the ability to accept chip-enabled cards at the register (Marcus, 2018). Despite this, increasing security investments does not equate to a corresponding increase in Incredibly robust security infrastructure in today's complex and evolving security environment. Organizations such as universities must adopt effective data security measures strategies to complement huge investments that are being made to mitigate or prevent data security threats (Marcus, 2018). According to He et al. (2020), when identifying cybersecurity strategies, demonstrating proactiveness, providing clear direction, establishing business objectives, business alignment, and intelligent decision-making are some of the tenets of effective cybersecurity strategies.

An intelligent computing approach based on group intelligence to secure the information of virtual users provides an additional layer of protection for systems that are not fully secure (Tan & Yu, 2018). As Tan and Yu (2018) reported, the algorithmic model is designed to collect the historical data of a visitor's access to private information. This way, the threshold settings can be augmented to protect the user's data adequately.

Filters for email messages is a vital strategy to prevent phishing attack. To start addressing this issue, universities should set up email filters that automatically forward suspicious emails from non-universities to users' spam folders as a first, simple step (Banerjee et al., 2022)**.** Even though this is not a foolproof method of fixing the problem, it is still an essential first step toward preventing malicious emails from reaching their intended recipients.

Employee security training is one of the most effective ways to prevent cyberattacks. Educating employees about security threats will help them identify and respond effectively (Banerjee et al., 2022). A simple way to avoid a data breach due to human error is to make employees aware of common attacks, such as phishing emails (Islam et al., 2018). University training programs should teach end users what phishing is and how to recognize it, and must commit the time and resources necessary to provide faculty and staff members with the education they need to be successful (Banerjee et al., 2022). According to He et al. (2020), users should be exposed to various phishing attacks during this training. In addition to providing examples of actual attacks, creating a repository that combines all such attacks, as Princeton University has done with its "Phish Bowl," can be beneficial (He et al., 2020).

Installing a firewall and threat detection software is another strategy for universities to prevent cyberattacks (Wu et al., 2022). Firewalls and other threat detection systems that monitor organizational network traffic, such as endpoint detection and remediation (EDR) solutions, can identify abnormal activity within the network (Wu et al., 2022). As a firewall, it is one of the most effective methods of creating a barrier between untrusted external networks and secured internal devices (Bakhsh et al., 2019). Threat detection software and other EDR solutions detect and eradicate possible Malware (Bakhsh et al., 2019).

Universities could prevent cyberattacks by installing updates and security patches regularly. It is crucial to close security gaps as soon as possible to prevent cybercriminals from exploiting weaknesses in unpatched or outdated software (Wu et al., 2022). Besides, an effective patch management schedule will mitigate the cyber risk associated with the university information systems by identifying vulnerabilities within the network, glancing for patches available, and systematically installing those patches on all relevant assets within the network (Bakhsh et al., 2019).

In today’s world, people cannot manage the increasing attack surface and process the high capacity of vulnerabilities evolving daily without support (Dasgupta et al., 2022). Several cyber security automation tools are available for universities to implement to automate cyber risk prevention processes. These tools, such as cyber asset attack surface management, risk-based vulnerability management, and cyber risk quantification, are designed to allow security teams to work efficiently and at scale (Dasgupta et al., 2022).

Assessing university cyber risks helps determine the impact of cyber threats across its networks, devices, applications, and users (Ali & Mohd Zaharon, 2024). Evaluating risk profiles can also serve as a valuable tool for identifying how adequate existing security controls are and where coverage gaps may exist (Dasgupta et al., 2022). There are several advantages to conducting a cyber risk assessment, including obtaining an accurate overview of the university attack surface by identifying areas of vulnerability that can be exploited (Ali & Mohd Zaharon, 2024). It also helps the university cyber team determine which vulnerabilities need to be prioritized so that they can be resolved as quickly as possible.

In summary, cyberattacks threaten universities, their customers, and the global economy by infiltrating and stealing vital and confidential information for personal and illegal benefit (He et al., 2020). Many themes in the present research emphasize cyberattacks and security related to organizations. Shlomo et al. (2021) quoted financial data losses in retail organizations such as Target, Neiman Marcus, and Michaels. Alraja et al. (2023) deliberated the Sony network’s attacks to disrupt service and personal information theft as another theme for data breaches. Cameroon University’s database was hacked, and examination results were altered (Boraine & Doris, 2019). Managing personal data has become an issue in universities because they hold rare data. There continues to be significant data loss as breaches occur more often, affecting data security and damaging network integrity and business reputation (Boraine & Doris, 2019)

The rise in cyberattacks that compromise private and organizational data shows no signs of slowing down as university institutions’ increased development of technologies and dependence on the Internet corresponds with the growth in cyberattacks (Rahim et al., 2019). There is a gap in research about the lack of active cybersecurity measures and security culture within university institutions (Rahim et al., 2019). This study obtained evidence from systems theory to support effective strategies to prevent cyberattacks within universities. Systems theory describes the principle that a system’s parts can best be understood in the context of the relationships with each other and other systems rather than in isolation (Adams et al., 2014; Bertalanffy, 1968). Using the system theory in this study is expected to give me a means for developing an in-depth identification and understanding of the participants’ strategies for mitigating the incidences and costs of cyberattacks

University IT leaders are responsible for ensuring the safety of online services for students, faculty, and staff. Universities are expected to safeguard their customers’ private information by providing a secure and inaccessible database to unauthorized users. The assumption remains that these systems are under siege, and reports of systems under attack remain common within the university environment. To prevent cybercrime at universities, university IT leaders must become aware of the risks associated with cyberattacks directed at their institutions. The organization may be required to work with students, faculty, staff, and visitors to promote safe Internet practices, provide encrypted and secure transactions as a standard business practice, and, most importantly, protect the institution’s integrity by ensuring consumer data is protected, unethical practices are avoided, and reputation is protected (Rakas et al., 2020). Universities are doing their part to combat these issues. Still, suppose we dig deeper into what effective strategies IT leaders employ to protect our institutions from cyberattacks. In that case, we may provide some solutions that would help protect the increasing number of academic institutions that do not have a strategy or the capability to prevent cyberattacks.

Transition

Section 1 contained an introduction to the study regarding effective strategies university information technology leaders use to prevent or mitigate cyberattacks’ costs. Section 1 included the background of the study, the problem and purpose statement, the nature of the study, the research question, interview questions, and the conceptual framework. In addition, I included the assumptions, limitations, and delimitations, the significance of the study, and the literature review for the study. Reviewing previous research allowed me to discover what information exists concerning the survey. Reviewing the academic and professional literature also allowed me to compare sample sizes, research methods, and designs. Section 2 contained an overview of the purpose statement, the role of the researcher and participants, and an explanation of the methodology, research design, and data collection techniques that I used as the researcher. Population and sampling, ethical research, data collection, data organization, data analysis, and reliability and validity methods concluded Section 2. Section 3 includes an introduction, presentation of findings, application to professional practice, implications for social change, recommendations for action, further research, reflections, and conclusion.

Section 2: The Project

In this study, I aimed to identify and explore the effective strategies that IT leaders of universities in Cameroon use to prevent or mitigate the costs of cyberattacks. Section 2 includes the (a) purpose statement, (b) role of the researcher, (c) participants, (d) research method, (e) research design, (f) population and sampling, (g) ethical research, (h) data collection instrument, (i) data collection technique, (j) data organization, (k) data analysis, and (l) reliability and validity. The section ends with a transition to Section 3.

Purpose Statement

The purpose of this qualitative pragmatic inquiry was to explore the effective strategies IT leaders of universities in Cameroon use to prevent or mitigate cyberattack costs. This study's population comprised eight IT leaders from universities in Cameroon with more than 5 years of experience in cybersecurity management and used effective strategies to prevent cyberattacks. IT leaders were suitable participants for this study because of their knowledge and experiences in preventing and mitigating cyberattacks. This study's findings could be valuable to IT leaders and cybersecurity professionals to plan and implement effective strategies to prevent cyberattacks. This study's findings may contribute to a positive social change by giving university IT leaders confidence and the necessary procedures to safely secure students' and staff's sensitive data and improve the economy's health. Furthermore, positive social change can result from providing a safe and secure learning environment for universities to conduct daily business activities.

Role of the Researcher

As a principal instrument in qualitative research, the researcher plays a central role (Leedy et al., 2019). The researcher collects and analyzes data to report the findings (Merriam, 2019). As the researcher, I played a fundamental role as an instrument in this study to the data collection, analysis, and report of the study findings. There is a possibility that researchers can decrease their personal bias by sharing their connection to the research project (Paxton, 2020). My current professional career as an IT specialist gives me a unique link to the study. I have worked as an IT professional for more than 10 years. In my career, I have experienced personal security breaches. I have extensive cybersecurity experience, including threat analysis, configuring security tools, defining and monitoring access privileges, and overseeing and monitoring route security administration. This work experience helped me understand what the participants said about cybersecurity.

Researchers must also adhere to ethical behavior to maintain scholarly work and protect study participants. The 1979 *Belmont Report* is one model that focuses on human subject research (Pritchard, 2021). This report is based on three values: respect for persons, beneficence, and justice (Pritchard, 2021). The necessity for ethical practices cannot be neglected in social science because human subjects are the center of any investigation in this field. Scientists should perceive the *Belmont Report's* values by using informed consent, exploiting benefits over risks, and considering who benefits and who is impaired (Mthunzi et al., 2020).

My responsibility was to reduce prejudice and avoid creating unbiased opinions through some reactions. Specific measures must be taken to maintain a positive relationship with participants, ensure reliability, and minimize bias in the data collection and analysis process (Yin, 2018). Triangulation, member checking, and outlining the data collection process can reduce bias in qualitative research; however, all biases cannot be eliminated (Kern, 2018). In this study, I used member checking, defined the data collection process, and used methodological triangulation to minimize bias. Furthermore, researchers can reduce the risk of bias by following the interview protocol (Yin, 2018). The interview protocol comprises the interview questions and the script to guide the interviewer in the interview procedure. I used an interview protocol (see Appendix) to navigate the data collection process. The semistructured interview protocol was suitable for this study because semistructured interview protocol offers convenience and flexibility in data collection by permitting interviews to be carried out on several platforms, such as face-to-face, telephone, zoom, and WebEx (Yin, 2018). Consistency in data collection indicates the phenomena under investigation are explored thoroughly, and flexibility in data collection and questioning supports the need for a standardized set of open-ended questions and a semistructured interview protocol (Yin, 2018). This study interview protocol included open-ended questions that engaged participants in discussing the study's overarching research question (Creswell & Creswell, 2018), follow-up questions, and probes for clarification or elaboration. Every participant had to answer all the interview questions to maintain consistency.

Participants

This study's case subjects were universities in Cameroon. This study's participants comprised eight IT leaders, security managers, and CIOs with more than 5 years of experience in cybersecurity management and used effective strategies to prevent cyberattacks. These participants were significant in addressing the research problem because university institutions assume an abundance of cybersecurity policy compliance. The researcher should select participants appropriate to the study to enhance the data collection process and answer the research question (Geng et al., 2021). I chose participants who answered the research question in this study by identifying and exploring university IT leaders' strategies to prevent or mitigate the costs associated with cyberattacks; IT leaders, security managers, or CIOs contributed to this study because they manage cybersecurity functions in their respective institutions. To participate in this study, the individual had to know what the university has done in cybersecurity management and should not be less than 25 years of age.

After I received the IRB approval, I started the recruitment process. I used Google search engines and social media such as Facebook and LinkedIn to recruit participants who aligned with the study criteria and could consider the study findings helpful. I continued selecting individuals until I reached enough agreeable participants that met the determined sample size and achieved data saturation. Six participants per group is the minimum number to enter the data saturation point in a typical qualitative study (Creswell & Creswell, 2018). I interviewed a total of eight participants and reached data saturation.

Researchers must establish trustworthiness with participants before accessing them, receiving consent, and securing an agreement (Cassell et al., 2020). As initial contact, I sent invitation emails to the identified individuals using the contact information from the Google search engine or social media profile (Facebook and LinkedIn). The invitation email included a detailed description of the purpose of the study. Providing potential participants with a clear and precise description of the study's purpose increases trustworthiness (Leedy et al., 2019). The inclusion criteria for participants in the study included individuals with 5 years of experience in cybersecurity management who used effective strategies to prevent cyberattacks. The individual also had to be familiar with what the university has done for cybersecurity and not be under 25 years old.

Selecting individuals from the sample frame allowed purposeful sampling because I may initially have contacted the wrong individuals. Purposeful sampling permitted recommendations to add more participants (Yin, 2018). This sampling technique assisted me in reaching the appropriate persons best suited for an interview instrument. This study identified and explored the strategies IT leaders of universities in Cameroon use to prevent or mitigate the costs of cyberattacks, and exploration was attended as referrals to competent persons were established.

Research Method and Design

Research Method

The research methods researchers use include qualitative, quantitative, and mixed methods (Yin, 2018). I used the qualitative method for this study. Researchers use the qualitative approach to describe the phenomena under study (Yin, 2018). The qualitative method was suitable for this study because I sought to identify and explore effective strategies that Cameroon university IT leaders used to prevent or mitigate the costs of cyberattacks. A qualitative approach is appropriate when a thorough understanding of an issue is necessary (Andrews, 2021). Addressing the research question required an in-depth analysis of the participants' experiences. The qualitative approach was appropriate for this study because it enabled the researcher to gather participant data through individual interviews.

Researchers use the quantitative method to test hypotheses or examine the relationships among variables (Huyler & McGill, 2019). The quantitative approach was unsuitable for this study because the intent was not to test any hypothesis or examine any relationship among variables. Researchers use the mixed method when the research question, objective, and context require hypothesis testing and an in-depth analysis of participants' experiences (Sim, 2020). The mixed method approach was unsuitable for this study because the research question, objective, and context did not require such an approach.

Research Design

Some of the qualitative research designs researchers use include pragmatic inquiry, ethnography, phenomenology, and narrative designs (Johnson & Christensen, 2020). I used a pragmatic inquiry design for this study. Researchers use pragmatic inquiry to answer *what, how,* or *why* research questions (Ridder, 2020). Pragmatic inquiry enables researchers to determine the reasons for a phenomenon through interviews, participants' observations, and field notes (Kelly & Cordeiro, 2020). Additionally, pragmatic inquiries are a method for eliciting data through introspection using semistructured interviews and thinking-aloud protocols to enable researchers to gain insight into participants' perceptions of their actions (Makin, 2021). The pragmatic inquiry design was appropriate for this study because it is an inductive approach that allowed me to identify, explore, and compare the effective strategies IT leaders of universities use to prevent or mitigate the costs of cyberattacks. A natural environment allowed participants to express their views and thoughts (see Kelly & Cordeiro, 2020).

Researchers use the ethnographic method to understand how behaviors reflect a group's culture (Institutional Ethnography, 2020). The ethnographic design was not suitable for this study because the intent was not to study the behavior and culture of participants in this study. Researchers use a phenomenological design to understand lived experiences from a participant's perspective (Balikçi, 2022). The phenomenological design was unsuitable for this study because I did not plan to study the lived experiences of people or groups of individuals. I used the pragmatic inquiry for this study to identify and explore the strategies IT leaders of universities in Cameroon use to prevent or mitigate cyberattack costs.

Population and Sampling

This study's population comprised eight IT leaders, IT Managers, and or CIOs from universities in Cameroon who met the participant criteria: (a) IT leader, security manager, or CIO with more than 5 years of experience in cybersecurity management, (b) used effective strategies to prevent cyberattacks, (c) familiar with what the university has done in cybersecurity management, and (d) not less than 25 years of age.

In qualitative research, purposeful sampling is one of the most commonly used methods (Campbell et al., 2020). Purposeful sampling refers to a small sample from a larger population to collect data (Yin, 2018). I used purposeful sampling to recruit participants who met the study inclusion criteria in this study. Selecting individuals from the sample frame allowed purposeful sampling because I may initially have contacted the wrong individuals. Purposeful sampling allowed me to address the research question and permitted recommendations to add more participants. This sampling technique assisted me in reaching the appropriate persons best suited for an interview instrument. This study identified and explored the strategies IT leaders of universities in Cameroon use to prevent or mitigate the costs of cyberattacks, and exploration was attended as referrals to competent persons were established.

Data saturation occurs when no more new themes emerge from the researchers' collected data (Guest et al., 2020). Researchers using qualitative methods are more likely to reach data saturation when they select the proper sample size for their studies. Through purposeful samples and the interviewing of participants, researchers can reach data saturation. I used Google and social media (Facebook and LinkedIn) to collect the contact information of potential participants with the title of an IT leader, IT manager, or CIO on their profile. I continued selecting individuals until I reached enough agreeable participants that met the determined sample size and achieved data saturation. I interviewed at least eight participants and then conducted a preliminary analysis. I added two additional participants to see if the other interviews yield new themes or notably different practices from what I have already found in the initial analysis. I continued this process until the additional interviews did not deliver crucial new information.

During qualitative research, interviews serve as a tool for collecting rich, in-depth data (Yin, 2018). A semistructured interview protocol was suitable for this study because semistructured interview offers conveniences and flexibility in data collection by permitting interviews to be carried out on several platforms such as face-to-face, telephone, zoom, and WebEx (Yin, 2018). This study interview included open-ended questions to engage participants in discussing the study's overarching research question (Creswell & Creswell, 2018), follow-up questions, and probes for clarification or elaboration. Every participant answered all the interview questions to maintain consistency.

Ethical Research

The 1979 *Belmont Report* is one model that focuses on human subject research (Pritchard, 2021). This report is based on three values: respect for persons, beneficence, and justice. The necessity for ethical practices cannot be neglected in social science because human subjects are the center of any investigation in this field. Mthunzi et al. (2020) suggested that scientists should perceive the *Belmont Report's* values by using informed consent, exploiting benefits over risks, and considering who benefits and who is impaired.

The role of ethics in this study could not be undermined. This study used human subjects as participants. The informed consent allowed participants to understand the purpose of this study better, what was expected of them and how their answers were used, the voluntary nature of the study, and the right to leave the study at any time. As a motivation to participants, each participant was presented with a copy of the final report in anticipation that the findings would assist them in further improving their strategies to prevent or mitigate cyberattack costs. Participants' privacy was critical because the semistructured interview comprised questions regarding institutional compliance with cybersecurity policies. Semistructured interviews were conducted over the telephone. The telephone interview allowed participants to schedule the time and location most convenient to them for the interview. Allowing participants to determine the time and place of the discussion addressed ethical privacy concerns because telephone calls were made at any location the participant desired. The telephone interviews helped minimize the effects of social desirability bias as the participants did not feel pressured to answer any question if overhead by others (Mthunzi et al., 2020). The main objective of the telephone interview was to provide participants with a conducive environment to deliver valuable information to the study.

I respected and protected the participants' confidentiality in this study. Though all the collected information was non-sensitive, any identifying information was deleted and replaced with codes. The results were published with no personal identifying information. In the reporting results, specific universities and respondents' names were removed, and the results focused on themes offered in the data, contrasting the identification of particular universities. All the collected data were stored on a password-secured storage device and destroyed five years after completing this study. The final study manuscript included the Walden IRB approval number 11-17-23-1168339 and its expiration date of November 16th, 2024. Participants' privacy was watchfully protected and respected throughout the research and after the study.

Data Collection Instruments

A data collection process refers to a set of activities researchers undertake to collect data to answer the research question (Vanderstraeten, 2019). In qualitative research, the researcher is the primary instrument for data collection (Yin, 2018). According to Yin (2018), data collection in a qualitative pragmatic inquiry occurs through researchers' and study participants' collaboration. In this study, I was the primary instrument in data collection.

I used semistructured interviews via telephone as the method of data collection. Qualitative data can be collected using semistructured interviews, which provide structure during the interview to allow the researcher to remain focused (Yin, 2018). I conducted semistructured interviews with open-ended questions to understand IT leaders' strategies at Cameroon universities to prevent or mitigate cyberattack costs. Participants could share their insights and experiences systematically and methodically using open-ended questions. I used member checking to improve the reliability and validity of the data collection process.

This study used a semistructured interview protocol (see Appendix A) to guide the interview. The semistructured interview protocol was suitable for this study because semistructured interview protocol offers convenience and flexibility in data collection by permitting interviews to be carried out on several platforms, such as face-to-face, telephone, zoom, and WebEx (Yin, 2018). Qualitative research aims to allow participants to express their thoughts and ideas without being restricted to a pre-defined question (Levitt et al., 2017). This study interview protocol included open-ended questions that engaged participants in discussing the study’s overarching research question (Creswell & Creswell, 2018), follow-up questions, and probes for clarification or elaboration. Every participant answered all the interview questions to maintain consistency.

In qualitative studies, it is crucial to review organizational documents to improve validity (Yin, 2018). As part of the study, I asked participants for any organizational documents on cybersecurity. I also searched for publicly available records on the university websites and social media pages.

Data Collection Technique

Data collection depends on the study’s methodology and approach to answer the research question. This study used the qualitative method because the focus of this study explored a real live phenomenon (Yin, 2018). The qualitative approach in this study necessitated me to be the primary instrument for data collection. As the primary instrument, I should know the qualitative methodology to gain credibility (FitzPatrick, 2019). I have conducted two qualitative research in the past: my past experiences in conducting qualitative research gave more credibility to the study.

I collected data from individuals who practice cybersecurity management. I used Google search engines and social media (Facebook and LinkedIn) to rebuild participants. I collected the contact information of potential participants with the titles IT leader, security manager, or CIO on their profiles. I continued selecting individuals until I reached enough agreeable participants that met the determined sample size and achieved data saturation. Creswell and Creswell (2018) indicate six participants per group as the minimum number to enter the data saturation point in a typical qualitative study. I send invitation emails to the identified individuals using their retrieved contact information in response to the recruitment e-mail campaign. I sent a follow-up e-mail to all individuals who responded positively and scheduled a screening call. Using the screening call script, I made a five to seven-minute screening call to every potential participant who reacted positively to the initial recruitment e-mail before participating in this study. The call aimed to introduce the research, ensure the participant met the criteria for partaking in this study, and explain the level of engagement, the risk involved, and the process for participating (Creswell & Creswell, 2018). I gave each participant an informed consent form. This consent form encouraged the interested persons to take the next step to participate in the study. It explained to participants the ethical standards for research expected from Walden University scholars. I asked all potential participants who choose to participate to submit an email with the word “I consent” in the subject line.

All participants who consented to participate received an e-mail correspondence that included a thank-you note for their willingness to participate in the study, confirming the interview date and time. I did not offer any payments to participants because this study was voluntary, and participants had the right to leave at any time. I searched participants’ institutional websites and social media pages for any publicly available information or documents on cybersecurity. I continued the recruitment process until the targeted sample size and data saturation were met.

This study’s data source included a semistructured interview and the analysis of publicly available documents on cybersecurity. An in-depth interview was the primary source of data collection in the qualitative study. It is considered valuable because of the ability to contribute toward retaining the power of flexibility. This flexibility helps gain insight and understanding of phenomena. I used semistructured interviews for this study because this type of interview structure permitted direct conversation with the participants to get a behind-the-scenes look at what was happening. Researchers used secondary data sources because secondary data sources are increasingly considered significant in qualitative study data collection. The secondary data source is vital in supplementing primary data sources; it provides a new perspective, creating grounds for comparison. This study's secondary data sources were publicly available documents on cybersecurity. This study collected non-sensitive data.

At the beginning of the interviews, I reminded the participants of their voluntary participation in the study, the right to leave at any time if necessary, and their answers should comprise only non-confidential information. I allowed participants to ask questions or concerns before giving informed consent. As part of the interview process, I verbally verified the informed consent before the interview and recording. The interviews were conducted at the scheduled suitability time for the participant. This semistructured telephone interview started with demographic questions and later with guiding questions, as revealed in the interview protocol (see Appendix A). Each of the interviews lasted from 25-40 minutes. As the primary instrument for data gathering, I guided the interview questions in a path that gave value to the study. According to Candela (2019), answering the study question requires exploration, and guiding interview questions could result in random data collection. I recorded the interviews using a digital recorder with the participant's authorization and took notes for participants who refused to authorize tape recording. I asked probing questions and requested clarification on incomplete and partial answers. At the closure of the discussion, I performed a transcript review by having participants verify the interview summary, minimize errors, and increase the study's credibility. Using semistructured interviews and the analysis of publicly available documents on cybersecurity as sources of data collection in this study aligned with the study's need because the research question wanted to explore how a process works and gain insight into the views and behaviors behind those processes. Other instruments like questionnaires could be applied to meet the objective, but the semistructured interview could potentially find unexpected results (Candela, 2019).

Data Organization Technique

The data I collected was organized to maintain the study's integrity so that the data can be accessed efficiently and securely. Several software programs, such as Zotero and NVivo, are available to qualitative researchers to organize notes, annotated bibliographies, and other research data (Leedy et al., 2019). Managing the transcribed data is an excellent way to increase the integrity of the data (Yin, 2018). This study used NVivo 14 to transcribe and code all the data collected during interviews. According to Alam (2020), NVivo is an innovative data analysis tool that supports idea management, data visualization, and data mining. NVivo supports more data formats than ATLAS, and MAXQDA, such as PDF files, audio files, word, excel, and more (Alam, 2020). I selected NVivo 14 because it could process interior and external data to the study database. Once I loaded the raw data into NVivo 14, I searched the data for themes. Grouping techniques helped me identify emerging data themes (Guest et al., 2020). In qualitative research, participants’ identities are protected through coding (Leedy et al., 2019). My coding process used letters and numbers to safeguard the confidentiality of the participants. I used a locked filing cabinet to store all the data. The information is not accessible to anyone else. After five years, I will shred physical documents and destroy electronic data using KillDisk software as mandated by Walden University IRB.

Data Analysis

Analyzing data in qualitative research involves methods for evaluating the study findings. A coding technique is used to observe patterns in the data (Leedy et al., 2019; Yin, 2018). In the pragmatic inquiry research process, the researcher often initiates the data analysis while collecting data. This study increased the reliability of the results by employing triangulation as a method of accounting. The use of triangulation refers to the process of analyzing data from multiple sources (Natow., 2020). This study’s secondary data sources were publicly available documents on cybersecurity. According to Natow (2020), using triangulation to enhance the validity of research questions is one of the methods used by qualitative researchers.

As Yin (2018) suggested, qualitative data can be analyzed in five steps: (a) compiling, (b) disassembling, (c) reassembling, (d) interpretation, and (e) conclusion. To analyze data in the study, I used Yin’s five-step method for analyzing data. The first phase of the research project was compilation; to compile data and information from other sources, I sorted and arranged field notes from different data resources (Yin, 2018). In the second phase of the process, I disassemble the data; this process is called disassembling. Yin (2018) suggests separating the original compiled data into smaller groups.

Reassembling was the third phase, in which I combined the data from Phase two to identify emerging themes (Yin, 2018). I used computer-based software to reconstruct the data as part of the reassembling process. Phase four was the interpretation of the reassembled data. This was the phase of the procedure whereby I interpreted the reassembled data (Yin, 2018). As a result of the interpretation, I had to disassemble the data or reassemble it in a new way to interpret it (Yin, 2018). According to Yin (2018), phase five is the study's conclusion. Based on the interpretation of the data in phase four, I concluded the whole research (Yin, 2018). Yin (2018) describes the five stages of assembling and reassembling data as iterative and reoccurring.

According to Leedy et al. (2019), a researcher should use triangulation to search for alternate data sources. In qualitative research, triangulation is a helpful validity strategy (Natow, 2020). My approach will be based on methodological triangulation. For data analysis in the study, I used the within method to conduct interviews and review the university documents to sustain my data analysis. To provide conclusive data, researchers use methodological triangulation to strengthen the validity of their findings (Natow, 2020).

In addition to other qualitative data collection methods, researchers use documentation analysis to demonstrate the correlation between two or more qualitative data collections (Leedy et al., 2019). The application of the various methods of data collection increased the chances of identifying similarities and discrepancies between the data. I used the comparative form to make comparisons. Comparative methods consist of grouping comparable themes into larger groups and comparing newly emerging themes; I reported findings and determined themes. To analyze and group the data collected, I used NVivo 14, a software program developed to organize and analyze data following the themes that emerge from the data collection process.

The participants' privacy was respected. I deleted all personal identifying information and replaced them with codes. In the reporting results, I removed specific institutional and respondent names, and the results were focused on themes offered in the data, contrasting the identification of particular institutions. I stored all the collected data on a password-secured storage device to be destroyed five years after the completion of this study.

Reliability and Validity

Reliability

The reliability of a qualitative pragmatic inquiry is contingent on the researcher's ability to gather data and perform data analysis (Leedy et al., 2019). As the primary instrument, I should know the qualitative methodology to gain consistency in study findings (Yin, 2018). To ensure the reliability of this study, I employed the triangulation strategy. In this strategy, I collected multiple forms of data related to the same research question to find consistencies or inconsistencies among data (Creswell & Creswell, 2018). These data forms included a semistructured interview and the analysis of publicly available documents on cybersecurity. I applied the member-checking strategy by presenting the preliminary analysis results to participants and getting feedback. I compared transcribed interviews with recorded interviews to enhance the data collection accuracy and the study’s reliability.

Validity

An appropriate methodology and analysis process must be used to establish sound results of a study to be valid (Natow, 2020). The methodological triangulation of data from multiple sources, member checking, and peer debriefing has been mentioned by Quintão et al. (2020) as methods for improving the validity of qualitative research. It has been demonstrated by Creswell and Creswell (2018).) that it is essential to triangulate when conducting qualitative research to ensure that various sources are used to determine the validity of any conclusions that can be made about a phenomenon. During the member-checking process, participants are asked to review their contributions to the study, update any misinformation they may have provided, and answer any questions. As a result, the research becomes more valid by ensuring that the interview data collected is appropriately interpreted. To ensure the study’s validity, I used a combination of triangulation methodology and member checking.

Research credibility involves participants confirming that the researcher’s interpretation and presentation of the data are accurate (Motulsky, 2021). The process of member checking assists participants in creating credibility (Motulsky, 2021). The member-checking process occurs when a study’s findings are reviewed by the participants of the study (Y. Connolly & Wall, 2019). As part of my efforts to increase validity, I used the member-checking method to assess the results of my research. I requested participants to review my interpretations of their responses during the interview to ensure that I correctly captured their answers.

Quintão et al. (2020) recommend that researchers share their experiences as researchers and verify the findings with participants to demonstrate credibility. To increase qualitative credibility, Quintão et al. (2020) further recommend observing and taking notes during engagement. I shared my experiences and findings with the participants to establish credibility.

A researcher has reached data saturation when no new themes emerge while collecting and analyzing the data (Quintão et al., 2020) In the case of data saturation, researchers can identify redundancies and repetitions from the data they collect (Guest et al., 2020). As far as the sampling is concerned, I used a purposeful approach. In addition, I conducted interviews with participants until I collected repetitive and redundant data. According to Quintão et al. (2020), data saturation in a qualitative study is crucial to ensure validity, confirmability, credibility, and transferability.

Transferability

A recent study by FitzPatrick (2019) suggested that transferability may be similar to generalizability. According to Singh et al. (2021), generalization is difficult, but incorporating triangulation is one way to achieve generality. Transferability was incorporated in this study. I conducted and transcribed semistructured interviews and provided the interview protocol (Appendix A). Furthermore, I followed the guidelines of conducting a qualitative pragmatic inquiry and arrived at data saturation as I had repetitive themes and codes within my analysis. The process I used in my data analysis aligned with the data analysis technique advocated by Yin (2018).

Transition and Summary

In Section 2, I restated the purpose of the study, including a detailed description of the researcher's role, participants, research design, population and sampling, ethical research, data collection, data organization, data analysis, reliability, and validity. I also provided a detailed description of the data collection and analysis process.

As described in Section 2, I conducted semistructured telephone interviews with eight IT leaders who have used effective strategies to prevent or mitigate cyberattack costs. The interview aimed to exploit IT university leaders' effective strategies to prevent or mitigate the cost of cyberattacks. I attained data saturation and received access to some publicly available documents on cybersecurity on the institution's websites. I ensured all collected electronic data were secured with password protection. I exploited methodological triangulation to guarantee the data analysis and the reliability of the findings.

In Section 3, the findings of this research are presented, practical implications for professional practice are explained in more detail, and the impact on social change is also discussed in more detail. Section 3 also includes recommendations for several actions and suggestions for further research, which are grouped into the topics inside the study that require more in-depth investigation and may produce additional questions to help improve business practice. In addition, Section 3 covers my experiences during the research process, any biases or misconceptions I encountered during the process of predetermined thoughts and values, and finally, the conclusion statement.

Section 3: Application to Professional Practice and Implications for Change

Introduction

This qualitative pragmatic inquiry aimed to explore the strategies IT leaders use to prevent or mitigate the cost of cyberattacks effectively. The conceptual framework that grounded this study was systems theory. Data were collected from eight participants, including IT leaders, IT managers, and CIOs, and four institutional documents were analyzed using thematic analysis. In the data analysis process, three main themes were identified: (a) employment of multiple strategies, (b) educational training, and (c) adopted policies and procedures. Relating the study's findings to system theory, some university IT leaders use multiple strategies to prevent or mitigate the cost of cyberattacks.

Presentation of the Findings

This study's overarching research question was "What strategies do information technology leaders in Cameroon universities use to effectively prevent or mitigate the costs of cyberattacks?" The data sources in this study included semistructured interviews with eight participants from universities in Cameroon and four institutional documents on cybersecurity. After completing a total of eight interviews, no new ideas or themes were generated, signifying that I had reached data saturation. Participants were allocated unique pseudonyms, and data collected during interviews were transcribed and named accordingly to maintain confidentiality, as shown in Table 2. NVivo 14 was used to organize the collected data and conduct a thematic analysis. Three main themes were identified based on the participant's responses to the interview questions, as shown in

Table 3. The first theme was that IT leaders effectively employ multiple strategies to prevent or mitigate the cost of cyberattacks. The second theme that emerged was educational training, and the third theme identified was the adoption of security policies and procedures to address cyberattack issues.

Table 2

Interview Specifications

Interview	Pseudonym	Transcript ID
Participant 1	P1	P1
Participant 2	P2	P2
Participant 3	P3	P3
Participant 4	P4	P4
Participant 5	P5	P5
Participant 6	P6	P6
Participant 7	P7	P7
Participant 8	P8	P8

Table 3

Key Themes

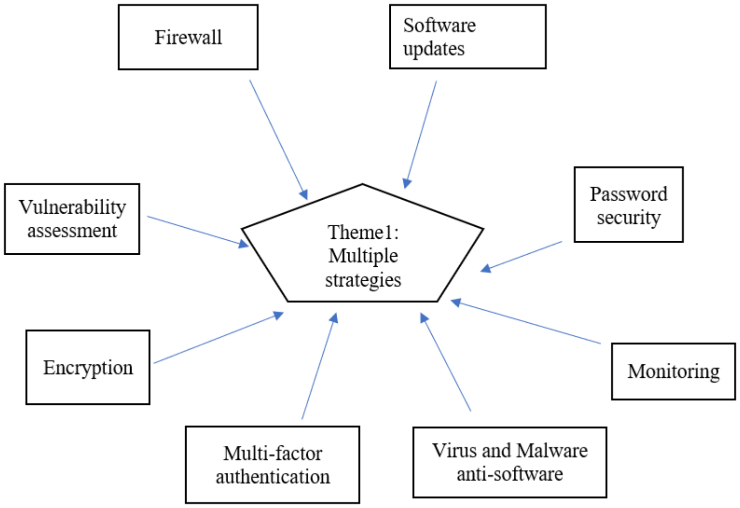
Themes	Sources	References
Employ of multiple Strategies	8	32
Educational training	8	22
Adopted policies and procedures	8	25

Theme 1: Employment of Multiple Strategies

The IT leaders interviewed in this study described employing multiple strategies to effectively prevent or mitigate the cost of cyberattacks in their institutions. This theme answers the research question directly. The various codes that contributed to this theme in addressing the research question are shown in Figure 3.

Figure 3

Contributing Codes to Theme 1


Firewall
Software updates
Vulnerability assessment
Password security
Theme1: Multiple strategies
Encryption
Monitoring
Multi-factor authentication
Virus and Malware anti-software

The participants deliberated eight effective strategies used to prevent or mitigate the costs of cyberattacks, as described in Table 4.

Table 4

Participants Use Multiple Strategies

Strategy	Description	Participants
Firewall	Firewalls are security devices installed on networks that filter traffic from the internet to the network. Based on the rules set, it blocks or allows traffic according to the restrictions set (Kim et al., 2020).	P1, P2, P3, P6
Software update	As a result of outdated software, a system is vulnerable to cyberattacks due to vulnerabilities in the software (Chigada & Madzinga, 2021).	P3, P6, P8
Password security	Password security ensures that no one else can access each user’s identity without their password (Dupuis et al., 2021).	P1, P2, P3, P4, P5
Monitoring	A monitoring system and its implementation can help mitigate the growing risks associated with cyberattacks (Salahdine & Kaabouch, 2019).	P1, P2, P6
Virus and malware anti-software	Software that detects viruses and malware looks for patterns based on their signatures or definitions. It is essential to keep your computer updated with the latest updates from anti-virus vendors (Chigada & Madzinga, 2021).	P1, P6
Multi-factor authentication	Users provide two different authentication factors to verify their identity when using two-factor, two-step, or dual-factor authentication (Kim et al., 2020).	P6, P7, P8
Encryption	Encryption is a means of protecting data against the theft, alteration, or compromise of data and works by scrambling data into a secret code that can only be unlocked with the unique digital key that was created during encryption (Madhuri & Prabhu, 2023)	P1, P6
Vulnerability assessment	Vulnerability assessments are systematic assessments of an information system’s security weaknesses. The vulnerability assessment assesses the system’s vulnerability in terms of severity levels, recommends remedies, and provides recommendations for resolving the vulnerability (Dupuis et al., 2021)	P6, P8

Firewall

Firewalls are security devices installed on networks that filter traffic from the internet to the network. Based on the rules set, it blocks or allows traffic according to the restrictions set (Kim et al., 2020). Firewalls serve as a defense layer that permits IT leaders to stay visible on the network traffic. Four participants (P1, P2, P3, and P6) insisted on installing a firewall on the system. Firewalls are, therefore, vital security mechanisms that participants establish to monitor their systems, thereby helping to protect or mitigate the rising risks of cyberattacks. P1 reported, “We employ a multitiered approach to cybersecurity, which includes incorporating robust network security measures such as firewalls that stop untheorized individuals or hackers from getting in our systems.” P2 added, “we try to use some firewalls on our systems to stop scammers who claim to be government officials who can guarantee contracts, commissions.” P3 emphasized, “We also install some firewalls to prevent some attacks from all these cyberattackers.” P6 added, “Implementing robust like firewall and network segmentation to limit lateral movement in case of a breach.”

Software Update

Three participants (P3, P6, and P8) described keeping software up-to-date as essential cybersecurity practice. As a result of outdated software, a system is vulnerable to cyberattacks due to vulnerabilities in the software (Chigada & Madzinga, 2021). Participants emphasized the necessity for regular software updates. P3 said, “What I’ve been using over the years is mostly updating everything. We keep all the software up to date with all current updates.” P6 also noted, “We conduct regular vulnerability assessments and promptly apply security software patches.” P8 reported that they remove unnecessary or unexpected hardware from the network and update all software regularly, making it difficult for attackers to penetrate the system. Therefore, another security mechanism that university IT leaders use to prevent or mitigate the cost of cyberattacks is regular software updates.

Password Security

Password security ensures that no one else can access each user’s identity without their password (Dupuis et al., 2021). Cybersecurity experts have suggested that a good password should contain at least 10 characters with a combination of uppercase lowercase letters, numbers, and special symbols (Curry et al., 2019). The practice of strong passwords and regular password reset was one primary recommendation from the participants (P1, P2, P3, P4, and P5). According to researchers like Pearman et al. (2019), passwords should be reset every 60 days. P4 also supported this: “The first layer of defense that goes far as proactive is resetting password every 60 days.” P4 recommended password management training be adopted as a standard. P4 explained, “it can be password management in terms of this part of management; it can easily promote the users of strong, unique passwords and important regular updates. And also, it can be considered implementing a multifactor, multifactor application in terms of added security.” P3 added, “To prevent the cyberattackers from gaining access to whatever information we have, we use passwords and change them regularly.” P1 and P2 also advocated for the use of the password to prevent cyberattacks. P2 explained, “we try as much as possible to create strong passwords and change them regularly.” P5 emphasized, “Okay. The thing we use most is that we try as much as possible to protect our data through the use of passwords.” Based on these findings from participants’ responses, satisfactory password performances that include implementing strong passwords and regular password reset assist in preventing or mitigating the cost of cyberattacks.

Monitoring

A monitoring system and its implementation can help mitigate the growing risks associated with cyberattacks (Salahdine & Kaabouch, 2019). Three participants (P1, P2, and P6) stressed the importance of system monitoring as an effective control mechanism to prevent or mitigate cyberattacks. P2 explained,

> we use some systems to monitor. We use some programs and software to monitor our systems to make sure that in real-time or at every given time at the twenty-four hours clock, we always have people monitoring the system to see what’s happening in the background, who’s trying to assess the portal or something like that.

P1 responded, “We monitor the university website and update the website regularly.” P1 noted the effectiveness of the system monitoring approach. P1 said, “Our strategies are effective in some ways, which include regular monitoring and incident response protocols, which have allowed us to detect and neutralize the potential attacks, and we regularly assist the effectiveness.” P6 emphasized, “Utilizing intrusion detection and prevention systems to monitor and respond to suspicious activities.” These findings indicate that some university IT leaders use system monitoring to prevent or mitigate cyberattacks.

Virus and Malware Anti-Software

Another method discussed by participants to prevent attacks was software that detects viruses and malware. This software looks for patterns based on their signatures or definitions. It is essential to keep the computer updated with the latest updates from anti-virus vendors (Chigada & Madzinga, 2021). Two participants (P1 and P6) iterated the importance of installing anti-software. P6 said, "We employ advanced endpoint protection solutions and regularly update antivirus signatures. Anti-software is an essential component of cybersecurity," P1 added. "We also use endpoint security measures that include antiviral software and encryptions," P1 noted that using anti-software helps stop attacks on the systems. Therefore, installing anti-software aimed at viruses and malware is another technique some IT leaders use to prevent or mitigate cyberattacks.

Multi-Factor Authentication

The use of multi-factor authentication was another strategy discussed during the interview. The authentication process is a technique that prevents malicious actors from accessing organizational data. In the muti-factor authentication technique, users provide two different authentication factors to verify their identity when using two-factor authentication, also known as two-step or dual-factor authentication (Kim et al., 2020). Several participants (P6, P7, and P8) described the multi-factor authentication process as a practical approach to prevent attacks. P6 said, "Implementing strong access controls and multi-factor authentication to enhance user authentication." P7 suggested that using two-factor authentication helps prevent attacks by providing an extra security layer. P8 said, “We use two-factor authentication. We use a system called Acer where the user will log in on the phone, and a security code is sent to verify the user’s identity on the network.” Based on the study findings, two-factor authentication is used as an extra security layer to prevent or mitigate the cost of cyberattacks.

Encryption

Encryption was another one of the significant multiple strategies described by participants. Encryption is a means of protecting data against the theft, alteration, or compromise of data and works by scrambling data into a secret code that can only be unlocked with the unique digital key that was created during encryption (Madhuri & Prabhu, 2023). P1 explained, “We also use strong access control and data encryption to safeguard sensitive information.” P1 noted they have encryption standards to collect sensitive information. P6 added, “We use data encryption and enforce data encryption policies for sensitive information in transit and at rest.” According to the participants’ responses, encryption is a technique used to prevent or mitigate cyberattacks in the university environment.

Vulnerability Assessment

Vulnerability assessments are systematic assessments of an information system’s security weaknesses. The vulnerability assessment assesses the system’s vulnerability in terms of severity levels, recommends remedies, and provides recommendations for resolving the vulnerability (Dupuis et al., 2021). P6 reported, “Conducting regular vulnerability assessments and promptly applying security patches reduce the attack surface on our systems.” P8 emphasized,

> Regularly scan and take inventory of your network devices and software. Remove unnecessary or unexpected hardware and software from the network. Such hygiene contributes to cyber risk mitigation by reducing the attack surface and establishing control of the operational environment.

Based on the study's findings, vulnerability assessment is another control mechanism that some IT leaders use to prevent or mitigate the cost of cyberattacks.

Analysis of Theme 1 Under System Theory

The conceptual framework that grounded this study was systems theory. Systems theory has three main concepts: (a) system units, (b) interconnectivity, and (c) analyzing systems to enable a better understanding of interconnected systems (Adams et al., 2014; Bertalanffy, 1968). An essential element of systems theory is that it provides a theoretical basis for studying all systems in the context of an organization, and organizations are systems made up of subsystems that work together (Simola, 2018). A failure of one part of a system will result in the entire system not functioning as intended (Mar, 2019). In this study, systems units are the participant's system or network and the attacker or hacker trying to gain unauthorized access to the information or data maintained by university institutions. The second concept of systems theory is constant interconnectivity (Adams et al., 2014; Bertalanffy, 1968). In this study, participants discussed constant interconnectivity when discussing how one outdated software or device could alter the entire network or systems. Participants described how outdated devices or software could lead to unauthorized access to the organizational system.

Analyzing the system is the third concept of the systems theory. Participants addressed the idea of analyzing systems in Theme 1. Participants stressed the need to monitor the systems and users' authentications constantly. System monitoring enables the connectivity analysis between the attackers or intruders and the university network or devices. The system monitoring mechanisms consist of using two-factor authentication, strong passwords, password reset, constant updating software, and monitoring virus and malware anti-software. Therefore, in this study, participants demonstrated the features of systems theory when discussing the strategies used to prevent or mitigate the cost of cyberattacks. The study's findings indicate that each participant uses at least two methods to prevent or mitigate cyberattacks. Using a multiple-strategy approach to a problem is inherently a systems theory approach (Adams et al., 2014; Bertalanffy, 1968). The findings show that systems theory was the suitable conceptual framework for comprehending effective strategies to prevent or mitigate the cost of cyberattacks.

Comparison of Theme 1 to Existing Literature

In Section 1, I presented the literature review, where I outlined the IT strategies used by IT leaders to prevent or mitigate the cost of cyberattacks. One of the strategies was the installation of security software. Based on the findings of Pramanik et al. (2022), organizations that don't have an accurate listing of their software inventory are more likely to become a cybercrime target. This study's participants discussed employing firewalls, viruses, and malware anti-software. However, participants mentioned the high cost involved in deploying security software. The study findings are consistent with the literature, signifying that small non-profit organizations such as universities with limited resources are liable to increased risk of cyberattacks.

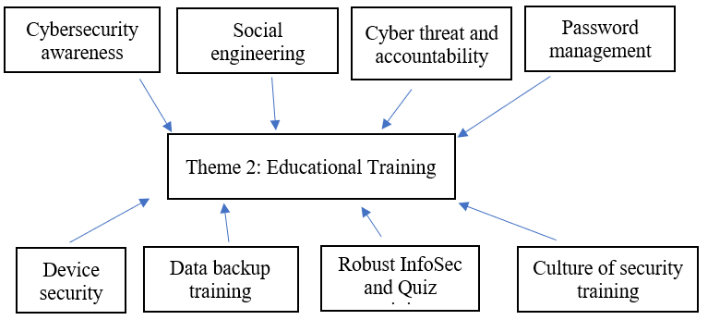
Furthermore, scholars such as Yu (2020) proposed that business leaders should prioritize email security to appropriately protect organizational, staff, and customer data. Email filtering was another strategy discussed in the literature. In this study, participants described email security in the context of creating strong passwords, multi-factor authentication, and resetting the password regularly.

Theme 2: Educational Training

The second theme identified from data analysis in this study was educational training. Participants discussed the importance of conducting educational training to create security awareness. Participants in this study addressed the importance of staff and student education to prevent or mitigate the costs associated with cyberattacks, which directly contributed to this study's research question. A number of codes contributed to the development of this theme, as shown in Figure 4.

Figure 4

Codes Leading to the Development of Theme 2



The participants described educational training programs as an essential strategy to prevent or mitigate the cost of cyberattacks. P1 and P6 described running educational training programs as crucial to preventing attacks. The training helps create cybersecurity and social engineering awareness for staff and students. P1 believed these educational training programs help to promote a security culture in the institution. P1 said,

> We conduct regular cybersecurity awareness training for our staff and students, focusing on patient prevention, password security, and engineering social engineering awareness. We also provide resources and ingredients to secure online practices and promote a culture of shared responsibility for cyber security. Mostly once per month.

P1 further emphasized that the educational training programs help to mitigate some of the challenges. P1 reported, “Major challenge that we encounter is the constant adaptation to the new and emerging threats in the cybersecurity dynamic field and also staying ahead of the evolving risks.” P6 added, “We conduct regular cybersecurity awareness training sessions for staff and students and provide specific training on recognizing phishing attempts and social engineering tactics. We also offer workshops on secure password practices and the importance of regular software updates.” P2 found it difficult for their staff and students to follow protocols, so they need educational training. P2 said,

> There are a lot of things we let our staff and students know. We make sure that the following protocol is a priority. We also have policies in place to keep sensitive data saved. We teach employees about cyber threats and accountability and try as much as possible to create strong passwords and change them regularly through password management training. Basically, there is no rigid timeframe for the training, but I would say we conduct this training from time to time. So, I would

> say twice, two times every month. And in the best-case scenario, we try to have these trainings thrice monthly.

P3 further emphasized the importance of educational training programs where staff and students are educated on identifying phishing emails and avoiding being victims of cyber theft. P3 said, “Use of seminars. For the seminar sessions, we create awareness. We also teach staff and students what is needed, what has to be done, what has to be known about cyber security, and how to be good at cyber security to avoid being attacked by cyberattackers. The seminars are every month.” P4 and P5 iterated on email security to protect institutional data and students’ and staff’s sensitive information. Through educational training programs, P4 can educate users on creating strong passwords, resetting passwords, and using multi-factor authentications to prevent unauthorized system access. P4 explained,

> I have so many various pieces of training for students and staff to enlighten them. Cybersecurity training can be password management; this part of management can easily promote the users of strong, unique passwords and important, regular updates. Also, it can be considered to implement multifactor applications in terms of added security. My second training is on device security. I know that in terms of this device, security can instruct users on securing their device, including keeping the operating system and software up to date and using anti-virus software.

P5 added, “We showed them how to back up the data and create strong passwords so cyberattacks cannot penetrate. We are just teaching them the basics. Trying to avoid issues like spamming, especially from email stuff like that," P5 believed that adequate educational training is the best course to prevent attacks. P5 said, "Well, I would say it's adequate training of staff and students. It's the best course of action. It makes everybody know what's happening, ways to prevent the issues from coming, and trying to avoid all those issues."

Other participants described educational training as a means to ensure information security best practices in the institution. P7 and P8 believed that successful cyberattacks could be significantly reduced if university institutions provided cybersecurity training for their employees and students. To prevent data breaches and other cybersecurity incidents, employees and students need to stay up-to-date on the latest threats and best practices for safeguarding sensitive information. P7 said, "We have our InfoSec training on day one." P8 emphasized, "We have cybersecurity training best practices for employees to prioritize following protocol, have policies that keep sensitive data safe, and teach employees about cyber threats and accountability. Create strong passwords and change them regularly. Enforce policies around payment cards and require backup of all essential data." Based on the study's findings, participants described educational training as a significant strategy to prevent or mitigate the cost of cyberattacks.

Analysis of Theme 2 Under Systems Theory

Incorporating educational training programs as an approach to prevent or mitigate the cost of cyberattacks, as described by participants, is a demonstration of the systems theory approach. Students, staff, devices, and applications are all crucial components of a system in information security (Pollini et al., 2022). The security of an organization's information is one of the most critical elements when meeting its long-term goals (Sepúlveda Estay et al., 2020) As a result, organizations such as university environments need to prioritize educational training programs to ensure that their infrastructure is protected against cyberattacks. By way of this, organizations can implement the systems theory principle of protecting their infrastructure against cyberattacks. As a result of cybersecurity training, employees will attain the basic knowledge required to recognize and respond to cybersecurity threats (He et al., 2020).

Based on the study's findings, it can be concluded that cybersecurity training should be prioritized as a strategy for implementing cybersecurity awareness within the workplace. The vulnerability of technology is as significant as the vulnerability of the people who developed it (Ani et al., 2019). Participants acknowledged that the importance of educational training could not be overstated and that each cybersecurity team member must be viewed as a contributory agent and a partner in the process. When one staff member or student fails to follow proper password hygiene, a risk can be spread to other devices or the entire system. Given this, the participants emphasize educational training as one of the most critical aspects of system theory regarding cybersecurity and cyberattacks in an applied environment such as a university.

Comparison of Theme 2 to Existing Literature

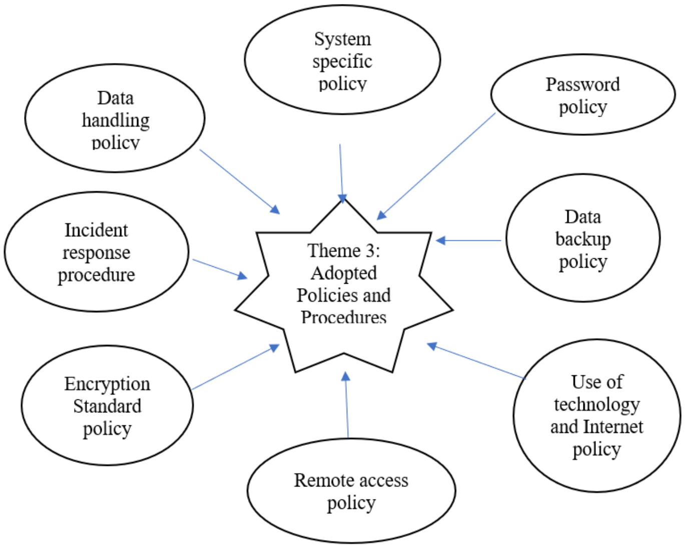
A significant focus of the literature on security was training employees in cyber awareness. Cybersecurity experts believe training employees on cybersecurity can help resolve the considerable weakness in any organization: human error. Employees can become the first line of defense against cyberattacks if they are fully aware of cybersecurity best practices and apply them in their everyday work (Buresh & Esq, 2022). A university's Information Technology (IT) leadership can customize training programs to meet the specific needs and priorities of the university.

Theme 3: Adopted Policies and Procedures

The last theme that emerged in this study was adopted policies and procedures. IT leaders interviewed in this study described adopting some policies and procedures to address cybersecurity issues in their institutions. This theme directly addresses the research question by providing IT leaders with contingency strategies to prevent or mitigate the cost of cyberattacks. The codes that led to the development of this theme are shown in Figure 5.

Figure 5

Contributing Codes to Theme 3


System specific policy
Password policy
Data handling policy
Data backup policy
Incident response procedure
Theme 3: Adopted Policies and Procedures
Encryption Standard policy
Use of technology and Internet policy
Remote access policy

By implementing a unified, comprehensive security policy, the hybrid network can automate and analyze security and network operations to a much greater extent. Organizations adopt this approach as a strategic initiative to orchestrate security-related changes across enterprise networks in a more informed, safe, and efficient manner (Alraja et al., 2023). Several participants described adopting some policies and procedures as strategic initiatives addressing their institutions' cybersecurity issues. P1 pointed out the importance of constantly updating policies and procedures to meet the needs of the changing security threats. P1 said, "We have clearly defined and regularly updated cybersecurity policies and procedures covering some areas, including data handling and incident response. The access control policies and the encryption standards are in place to collect our sensitive information." P1 emphasized, "We are continuously evaluating and, when necessary, upgrading our technology stack to ensure it aligns with the latest cyber security standards and collaboration with external partners and information sharing forums, which is a key to our strategy." P2 added, "We have identified the organization's security risk, assets, and threats while establishing password requirements. We provide designated email security measures and outline procedures to handle sensitive data. We set standards for handling technology, social media, and internet usage. And we also try to follow up our cyber security response plan."

The Internet of Things and social media pose a significant risk of cyberattacks to organizations (Aydos et al., 2019). Some participants described adopted policies and procedures as a strategy to mitigate the rising risks of cyberattacks.

P4 explained,

> First, I'll say that password Facebook policy in terms of this Facebook policy is

> an established requirement for creating management of passwords, including guidelines for complexity lines and frequency of data. I can also go into this data classification and handling policy to identify how different data types should be classified. It can be, for example, public sensitive confidential and prescribe the corresponding security measures for each particular reason. And also, I should go into remote assistance policies, which are also involved in government. The government should be able to secure and assist organizational resources from remote locations and detail the use of the vital private network, which is the VPN secure, the connection and application requirement. The last one should be employee training and awareness of the policy applied. When you’re trying to outline the organization’s commitment to ongoing cybersecurity training for employees, you should be able to promote awareness of potential threats and based practice.

P6 added,

> We have implemented an incident response plan procedure outlining steps in case of cyberattacks. We enforce data encryption policies for sensitive information in transit and at rest. We are establishing acceptable use policies for network and information system usage.

P8, like P2, has a data backup policy in place. Backup data is essential to restore systems in case of a cyberattack and ensure business continuity. P8 emphasized the importance of issue-specific policy that helps to address specific issues of concern to the institution and system-specific policy to guide the university administration’s decision in protecting particular systems. According to this study’s findings, to guarantee data security, it is vital to adopt policies and procedures that set out guidelines for various activities relating to data security, such as encrypting emails, limiting access to critical systems, and maintaining data integrity. As a result, it is essential to have policies and procedures in place due to the costs associated with cyberattacks and data leaks.

Analysis of Theme 3 Under Systems Theory

In theme 3, participants described the importance of policies and procedures to prevent or mitigate the costs of cyberattacks. Some of these policies and procedures discussed were the backup and password policies. According to Sepúlveda Estay et al. (2020), data security is critical to an effective organization. The fault of a single component of an organization’s security system can have a significant impact on the ability of the entire security system to function correctly (Palanisamy et al., 2020). The participant’s adopting policies and practices are consistent with systems theory. The participant who backed up data on each device or system in the network was able to understand the interconnected nature of the devices on the network by backing up their data. Continual backups of the data on individual devices provide a means of securing the data on the network in a protected or safe location, thereby preventing the loss of data in the event of a failure. Participants further discussed the importance of password policy, which includes using strong passwords, resetting passwords frequently, and using two-factor authentication. Participants noted their understanding of the interconnected nature of the system. A password weakness on one individual device could adversely affect other devices in a connected system. In this study, participants discussed constant interconnectivity when describing how a weak password on one device could alter the entire network or systems. Participants described how weak passwords or poor password management could lead to unauthorized access to the organizational system. Participants' views were based on analyzing the entire system rather than the individual device. These findings further show that systems theory was the suitable conceptual framework for comprehending effective strategies to prevent or mitigate the cost of cyberattacks.

Comparison of Theme 3 to Existing Literature

Security policies are noted in the literature as a primary control organization can implement to protect their data (Shields et al., 2020). Security policy is the primary enabler of processes within the organization and the continuous operation of information systems. Chapman (2021) suggests that the security policy serves as a document that lays out guidelines for maintaining security. Every employee within the organization is required to follow the same protocol. Employees who understand security policy can better act accordingly and be held accountable. Bansal et al. (2020) advocated including formal guidelines, monitoring procedures, and policy compliance methods. The literature strongly supports the importance of security policy; inadequate or insufficient implementation can weaken the information security process and render information security useless (Lee & Hong, 2020). IT leaders interviewed in this study described adopting some policies and procedures as strategic initiatives to address cybersecurity issues in their institutions. Organizations that adopt cybersecurity policies and procedures foster a culture of security awareness. Cybersecurity policies enable organizations to ensure that all employees are informed about best practices and their responsibilities. In addition to heightening awareness, this prevents human error from being the source of attacks and, in general, creates a safer work environment for everyone involved. It has been stated by Rostami et al. (2020) that implementing an information security policy plays a vital role in implementing system control. The study findings highlighted the significance of adopting security policies and procedures to ensure best practices and business continuity and prevent or mitigate the costs of cyberattacks.

Applications to Professional Practice

The study's findings have significant implications for the professional practice of IT leaders of universities in Cameroon in efforts to prevent or mitigate the costs of cyberattacks. Cyberattacks substantially threaten university institutions as universities increasingly rely on computer networks to conduct day-to-day business activities (Tayaksi et al., 2022). This subsection reports the study findings' application and makes a convincing theoretical argument on how these findings could improve business practices in information security.

Employ Inclusive Cybersecurity Strategies

The theme of employing multiple strategies to prevent or mitigate the cost of cyberattacks provides a vibrant directive to university IT leaders who operate in diverse cultural, national, and societal settings. Cyberattacks are increasing in universities in Cameroon. Threats such as the five information security incidents between 2015 and 2017 in Cameroon universities show that the sensitive information of students and faculty staff is at risk (Kessi et al., 2020). The theme highlights the significance of adopting a holistic cybersecurity strategy instead of relying only on a single security control measure. University IT leaders should implement robust authentication systems and data encryption techniques to enforce email protection. According to Purkait and Damle (2023), updating systems software, using a two-factor authentication method, and frequently resetting passwords reduce the probability of successful attacks on the system. Using multiple strategies is considered one of the best practices in the field of information security today (Ghelani, 2022). Therefore, university IT leaders of universities in Cameroon should employ multiple strategies to prevent or mitigate the cost of cyberattacks.

Making Educational Training Programs a Priority

The second theme that emerged from this study's findings was educational training, which emphasizes the importance of creating cyber awareness to reduce the rising risks of cyberattacks. Buil-Gil et al. (2020) noted human error as the primary cause of successful organizational cyberattacks. The overall lack of security awareness to mitigate human errors related to cybersecurity is directly linked to the rise of cyberattacks in Cameroon universities. IT leaders should prioritize security training for students and staff and educate them on recognizing phishing emails, social engineering, and password management. Students and staff can become the first defense layer against cyberattacks if they are fully aware of cybersecurity best practices and apply them in their everyday operations (Buresh & Esq, 2022). University IT leaders should customize training programs to meet the specific needs and priorities of the university.

Implementing Security Policies and Procedures

The study's findings stressed the importance of adopting policies and producers to create best practices to ensure business continuity and prevent or mitigate the cost of cyberattacks. By implementing a unified, comprehensive security policy, the hybrid network can automate and analyze security and network operations to a much greater extent (Alraja et al., 2023). Some participants in this study described adopted policies and procedures as a strategy to mitigate the rising risks of cyberattacks. Cameroon, had been a less developed country, lacked trained cybersecurity professionals to manage cybersecurity activities. It could adopt this approach as a strategic initiative to orchestrate security-related changes across enterprise networks in a more informed, safe, and efficient manner. University institutions increasingly rely on networks to conduct their day-to-day activities. However, the Internet of Things and social media pose a significant risk of cyberattacks to organizations (Aydos et al., 2019). University IT leaders of universities in Cameroon could reduce the rising threat of cyberattacks by adopting policies and procedures for best practices.

Implications for Social Change

This study's findings have thoughtful implications for lashing tangible improvements to individuals, communities, organizations, institutions, cultures, and societies, as the results could improve cybersecurity practices among university IT leaders of universities in Cameroon. Cameroon's unique cultural, economic, and political system significantly influences IT leaders' cybersecurity management. Identifying the several techniques IT leaders employ to prevent or mitigate the cost of cyberattacks empowers them to protect their institutions proactively. IT leaders could better defend their institutions by using multiple security control mechanisms and lowering the probability of successful attacks (Kipper et al., 2021). This study’s findings may contribute to a positive social change by giving university leaders confidence and the necessary procedures to safely secure students’ and staff’s sensitive data and improve the economy’s health.

Furthermore, making educational training programs a top priority will create awareness and a security culture within the institution. The findings also reveal that students and staff who are more educated can recognize and respond to possible attacks. Admitting the adoption of security policies and procedures to address cyberattacks explains the necessity for readiness in the corporate sector. Business leaders can protect business activities and uphold profit margins by implementing proactive and resilient measures to prevent or mitigate the costs of cyberattacks (Devi, 2023). These implications create a chance for social change as university IT leaders become change agents, providing a safe and better secure learning environment for universities to conduct daily business activities.

Recommendations for Action

IT leaders should use the results of this study as a basis for evaluating their current IT strategies to prevent or mitigate cyberattacks. In an effort to improve the cybersecurity in their organization, they must develop robust cybersecurity strategies and identify areas that could be improved. Using systems theory for analysis in this study, I recognized three significant themes that emerged from participant’s responses. In theme 1, the participants described employing multiple strategies to prevent or mitigate the cost of cyberattacks, incorporating educational training programs as theme 2. Lastly, in theme

3, participants identified adopting policies and procedures for best practices and business continuity to ensure adequate data protection. With the help of systems theory, the analysis of these study findings has been able to integrate these themes into a comprehensive set of strategies for preventing or mitigating the costs associated with cyberattacks, which should help reduce the risks involved in such attacks.

Threats such as the five information security incidents between 2015 and 2017 in Cameroon universities show that the sensitive information of students and faculty staff is at risk. University IT leaders in Cameroon should seek to use multiple strategies to prevent or mitigate the costs of cyberattacks. In a time when cyberattacks are becoming increasingly sophisticated and persistent, individual effort may be required to resist cyberattacks adequately (Susanto et al., 2021). Therefore, business leaders must build strategic alliances with other institutions to address their cybersecurity challenges effectively and proactively. Through collaboration, business leaders may be able to share and learn from each other’s expertise, experiences, and knowledge as they confront evolving cyber threats. Furthermore, employees are the first defense layer against cyberattacks, they must learn training programs and apply them in their everyday work (Buresh & Esq, 2022). Therefore, business leaders should strive to customize training programs to meet the specific needs and priorities of the university.

Recommendations for Further Research

This qualitative pragmatic inquiry addressing effective strategies used by university IT leaders in Cameroon to prevent or mitigate the costs of cyberattacks has offered significant insights into the cybersecurity practices of this particular group.

Nevertheless, other areas could benefit from further research to expand the knowledge in this field. The following recommendations are suggested for further research based on the assumptions and outcomes of this study.

It was assumed in the study that asking interview questions would produce rich, thick data that could be used to answer the research question. Interviewees responded to interview questions according to their own experiences. In order to confirm whether the findings from new research correspond to my conclusions, I recommend additional qualitative research studies involving organizations and different locations. This study had some limitations due to the small sample size used, which may not have allowed the results to be generalized to the business population at large. I recommend further research using a different design or method to determine if they can achieve the same results.

This qualitative pragmatic inquiry has codified a way for understanding the control mechanisms IT leaders of universities in less developed countries such as Cameroon use to prevent or mitigate the costs of cyberattacks. Further research should be conducted on various aspects of cybersecurity practices, the scope of the study should be expanded to larger organizations, and a mixed method should be used to develop effective cybersecurity strategies. Taking these recommendations into consideration and addressing them can dramatically improve the cybersecurity resilience of academic institutions and assist in protecting institutions, students, and staff from cyberattacks.

Reflections

I found the doctoral study one of the most thought-provoking academic endeavors I have ever undertaken. My research exposed me to a level of complexity I was unaware of before I began. It was not uncommon for me to spend several days, nights, and weekends reading books. The journey was also not without its obstacles; however, I managed to overcome them all. For me to achieve the goal of completing my doctoral journey, perseverance, discipline, and stamina were essential. A great deal of perseverance was required in order to overcome obstacles as they appeared. It took discipline for me to stay focused on writing rather than socializing with friends and family and spending time with them. During the course of my doctoral journey, I was able to stay on track because of my stamina.

The experience in this doctoral journey has also made me a better writer and researcher. I also gained a deeper knowledge of qualitative methods and pragmatic inquiry design as well. During my research, I was able to interview eight IT leaders who gave me a better understanding of the effective strategies university IT managers use to prevent or mitigate the costs of cyberattacks on their campuses. Despite my preconceived ideas about cybersecurity, I do not believe that my viewpoints prejudiced the views of the participants in the interview. It was a free-flowing exchange of cybersecurity experiences among the participants. Having knowledge of cybersecurity, I was able to ask probing questions to participants when required and clarify cybersecurity terms when necessary to improve the study findings.

Conclusion

This qualitative pragmatic inquiry using systems theory showed that university IT leaders employ multiple strategies to prevent or mitigate the cost of cyberattacks, prioritize educational training programs, and adopt policies and procedures to address cybersecurity-related issues. Using inclusive cybersecurity strategies, prioritizing educational training, and adopting policies and practices are crucial for IT leaders to protect their organizations from rising cyber threats. Furthermore, through collaboration, when business leaders build strategic alliances with other institutions to address their cybersecurity challenges effectively and proactively, business leaders may be able to share and learn from each other's expertise, experiences, and knowledge as they confront evolving cyber threats. This study's findings may contribute to a positive social change by giving university leaders confidence and the necessary procedures to safely secure students' and staff's sensitive data and improve the economy's health. Additionally, to expand the field of cybersecurity in the context of non-Western countries, further research should be conducted on various aspects of cybersecurity practices, the scope of the study should be expanded to larger organizations, and a mixed method should be used to develop effective cybersecurity strategies. Taking these recommendations into consideration and addressing them can dramatically improve the cybersecurity resilience of academic institutions and assist in protecting institutions, students, and staff from cyberattacks.

References

Adams, K. M., Hester, P. T., Bradley, J. M., Meyers, T. J., & Keating, C. B. (2014). Systems theory as the foundation for understanding systems. *Systems Engineering*, *17*(1), 112–123. https://doi.org/10.1002/sys.21255

Adebayo, D. O., & Ninggal, M. T. (2022). Relationship between social media use and students' cyberbullying behaviors in a West Malaysian Public University. *Journal of Education, 202*(4), 524–533. https://doi.org/10.1177/0022057421991868

Alam, M. K. (2020). A systematic qualitative case study: questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management An International Journal, 16*(1), 1–31. https://doi.org/10.1108/qrom-09-2019-1825

Alarifi, S. H. (2023). Small and medium businesses readiness towards cyberattacks in Saudi Arabia. *Global Economics Review, VIII*(I), 113–126. https://doi.org/10.31703/ger.2023(viii-i).11

Al-Ghamdi, M. I. (2021). WITHDRAWN: Effects of knowledge of cyber security on prevention of attacks. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.04.098

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform*, *33*(1), 101–121. https://doi.org/10.1177/10567879221082966

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, *129*.

https://doi.org/10.1016/j.cose.2023.103208

Andrews, S. (2021). Qualitative analysis at the interface of indigenous and western knowledge systems: The Herringbone stitch model. *Qualitative Research, 21*(6), 939–956. https://doi.org/10.1177/1468794120965365

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems & Information Technology, 21*(1), 2. https://doi.org/10.1108/JSIT-02-2018-0028

Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*, *38*(2), 218–226. https://doi.org/10.1177/0266666921997512

Aydin, H. (2021). A study of cloud computing adoption in universities as a guideline to cloud migration. *SAGE Open*, *11*(3). https://doi.org/10.1177/21582440211030280

Aydos, M., Vural, Y., & Tekerek, A. (2019). Assessing risks and threats with a layered approach to the Internet of Things security. *Measurement and Control*, *52*(5–6), 338–353. https://doi.org/10.1177/0020294019837991

Back, S., & Guerette, R. T. (2021). Cyberplace management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. *Journal of Contemporary Criminal Justice*, *37*(3), 427–451. https://doi.org/10.1177/10439862211001628

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programs for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ics-07-2018-0080

Bakhsh, S. T., Alghamdi, S., Alsemmeari, R. A., & Hassan, S. R. (2019). An adaptive intrusion detection and prevention system for the Internet of Things. *International Journal of Distributed Sensor Networks*, *15*(11). https://doi.org/10.1177/1550147719888109

Balikçi, A. (2022). Phenomenological research on the evaluation of teacher candidates from the perspective of school administrators. *International Journal of Contemporary Educational Research*, *6*(2), 468–482. https://doi.org/10.33200/ijcer.563490

Banerjee, S., Swearingen, T., Shillair, R., Bauer, J. M., Holt, T., & Ross, A. (2022). Using machine learning to examine cyberattack motivations on web defacement data. *Social Science Computer Review*, *40*(4), 914–932. https://doi.org/10.1177/0894439321994234

Bansal, G., Muzatko, S., & Shin, S. I. (2020). Information system security policy noncompliance: the role of situation-specific ethical orientation. *Information Technology & People, 34*(1), 250–296. https://doi.org/10.1108/ITP-03-2019-0109

Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L., & Koyuncu, M. (2022). Cybersecurity deep: Approaches, attacks dataset, and comparative study. *Applied Artificial Intelligence: AAI*, *36*(1). https://doi.org/10.1080/08839514.2022.2055399

Bertalanffy, L. (1968). *General systems theory: Foundations, development, application*. George Braziller.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020).

Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*. https://doi.org/10.1016/j.cose.2019.101677

Bicaku, A., Tauber, M., & Delsing, J. (2020). Security standard compliance and continuous verification for Industrial Internet of Things. *International Journal of Distributed Sensor Networks*, *16*(6), 743–748. https://doi.10.1177/1550147720922731

Boraine, A., & Doris, N. L. (2019). The fight against cybercrime in Cameroon. *International Journal of Computer (IJC)*, *35*(1), 87–100. https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1469

Bu, X., Zhao, X., & Yin, Y. (2023). Event-triggered model-free adaptive control for unknown multiple input and multiple output nonlinear system under denial-of-service attacks. *Journal of Vibration and Control: JVC*, *29*(21–22), 5123–5137. https://doi.org/10.1177/10775463221130819

Buil-Gil, D., Lord, N., & Barrett, E. (2020). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. In *SocArXiv*. https://doi.org/10.31235/osf.io/nd6xg

Buresh, D. L., & Esq, D. L. (2022). A simulation of how a cloud service provider from the Midwest should behave when faced with a potential cyber-attack, where many of its customers do business in the healthcare, banking, and educational industries. *Studies in Social Science Research*, *3*(4), 24. http://www.scholink.org/ojs/index.php/sssr/article/view/5211/6103

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing: JRN*, *25*(8), 652–661. https://doi.org/10.1177/1744987120927206

Candela, A. (2019). Exploring the Function of Member Checking. *The Qualitative Report*, *24*(3), 619-628. https://doi.org/10.46743/2160-3715/2019.3726

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & amp; Computer Security*, *27*(1), 101–121. https://doi.org/10.1108/ics-11-2016-0088

Cassell, C., Radcliffe, L., & Malik, F. (2020). Participant reflexivity in organizational research design. *Organizational Research Methods*, *23*(4), 750–773. https://doi.org/10.1177/1094428119842640

Cathcart, A. (2019). The secret war for China: espionage, revolution and the rise of mao. *War in History, 26*(2), 300–302. https://doi:10.1177/0968344518804624c

Chandna, V., & Tiwari, P. (2023). Cybersecurity and the new firm: surviving online threats. *The Journal of Business Strategy*, *44*(1), 3–12. https://doi.org/10.1108/jbs-08-2021-0146

Chang, S.-I., Chang, L.-M., & Liao, J.-C. (2020). Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. *Information & Management*, *57*(6), 103335. https://doi.org/10.1016/j.im.2020.103335

Chapman, P. (2021). Defending against insider threats with network security's eighth layer. *Computer Fraud & Security, 2021*(3), 8–13. https://doi.org/10.1016/S1361-3723(21)00029-4

Chatterjee, D. (2021). *Cybersecurity readiness: A holistic and high-performance approach*. SAGE Publications, Inc. https://doi.org/10.4135/9781071837313

Chigada, J., & Daniels, N. (2021). Exploring information systems security implications posed by BYOD for a financial services firm. *Business Information Review*, *38*(3), 115–126. https://doi.org/10.1177/02663821211036400

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1). https://doi.org/10.4102/sajim.v23i1.1277

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simulation & Gaming*, *51*(5), 586–611. https://doi.org/10.1177/1046878120933312

Cojocariu, A.-C., Verzea, I., & Chaib, R. (2020). Aspects of cyber-security in higher education institutions. In *Innovation in Sustainable Management and Entrepreneurship* (pp. 3–11). Springer International Publishing.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*(103614), 103614. https://doi.org/10.1016/j.compind.2022.103614

Creswell, J., & Creswell, J. (2018). *Research design: Qualitative, quantitative, and mixed* *methods*. Sage Publications.

Curry, M., Marshall, B., Correia, J., & Crossler, R. E. (2019). InfoSec process action model (IPAM): Targeting insiders' weak password behavior. *Journal of Information Systems*, *33*(3), 201–225. https://doi.org/10.2308/isys-52381

Dailey, S. L., Pierce, C. S., Bailey, D. E., Leonardi, P. M., & Nardi, B. (2023). Being creative within (or outside) the box: Bridging occupational identity gaps. *Management Communication Quarterly*, 089331892311673. https://doi.org/10.1177/08933189231167385

Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation Applications Methodology Technology*, *19*(1), 57–106. https://doi.org/10.1177/1548512920951275

Datta, P. M., & Acton, T. (2022). Ransomware and Costa Rica's national emergency: A defense framework and teaching case. *Journal of Information Technology Teaching Cases*, 204388692211490. https://doi.org/10.1177/20438869221149042

Davis, J., & Wilner, A. (2022). Paying terrorist ransoms: Frayed consensus, uneven outcomes & undue harm. *International Journal (Toronto, Ont.)*, *77*(2), 356–367. https://doi.org/10.1177/00207020221130308

Deng, J. (1982). Grey systems control. *Systems & Control Letters*, *1*(10), 288–294.

Devi, S. (2023). Cyber-attacks on health-care systems. *The Lancet Oncology*, *24*(4), e148. https://doi.org/10.1016/s1470-2045(23)00119-5

Dias, R. M., Zacarias, R. O., Varella, J. L. de L., & dos Santos, R. P. (2022).

Investigating information security in systems-of-systems. *XVIII Brazilian Symposium on Information Systems*. https://dl.acm.org/doi/10.1145/3535511.3535523

Dupuis, M., Jennings, A., & Renaud, K. (2021). Scaring people is not enough: An examination of fear appeals within the context of promoting good password hygiene. *Proceedings of the 22st Annual Conference on Information Technology Education*. https://dl.acm.org/doi/10.1145/3450329.3476862

Fawehinmi, O., Yusliza, M. Y., Wan Kasim, W. Z., Mohamad, Z., & Sofian Abdul Halim, M. A. (2020). Exploring the interplay of green human resource management, employee green behavior, and personal moral norms. *SAGE Open*, *10*(4), 215824402098229. https://doi.org/10.1177/2158244020982292

Feng, C. (qian), & Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*, *32*, 59–75. https://doi.org/10.1016/j.accinf.2018.11.001

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching & Learning*, *11*(2), 211–217. https://doi.org/10.1016/j.cptl.2018.11.014

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Geng, J., Du, W., Yang, D., Chen, Y., Liu, G., Fu, J., He, G., Wang, J., & Chen, H. (2021). Construction of energy internet technology architecture based on general system structure theory. *Energy Reports*, *7*, 10–17. https://doi.org/10.1016/j.egyr.2021.09.037

Ghelani, D. (2022). *Cyber security, cyber threats, implications and future perspectives: A review*. https://doi.org/10.22541/au.166385207.73483369/v1

Grewal, D., Hulland, J., Kopalle, P. K., & Karahanna, E. (2020). The future of technology and marketing: a multidisciplinary perspective. *Journal of the Academy of Marketing Science*, *48*(1), 1–8. https://doi.org/10.1007/s11747-019-00711-4

Greyson, D., Chabot, C., Mniszak, C., & Shoveller, J. A. (2023). Social media and online safety practices of young parents. *Journal of Information Science*, *49*(5), 1344–1357. https://doi.org/10.1177/01655515211053808

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PloS One*, *15*(5), e0232076. https://doi.org/10.1371/journal.pone.0232076

Hamilton, A. B., & Finley, E. P. (2019). Qualitative methods in implementation research: An introduction. *Psychiatry Research*, *280*(112516), 112516. https://doi.org/10.1016/j.psychres.2019.112516

Han, K., Choi, J. H., Choi, Y., Lee, G. M., & Whinston, A. B. (2023). Security defense against long-term and stealthy cyberattacks. *Decision Support Systems*, *166*(113912), 113912. https://doi.org/10.1016/j.dss.2022.113912

Har, L. L., Rashid, U. K., Chuan, L. T., Sen, S. C., & Xia, L. Y. (2022). Revolution of retail industry: From perspective of retail 1.0 to 4.0. *Procedia Computer Science*, *200*, 1615–1625. https://doi.org/10.1016/j.procs.2022.01.362

Hartnell, C. A., Ou, A. Y., Kinicki, A. J., Choi, D., & Karam, E. P. (2019). A meta-analytic test of organizational culture's association with elements of an organization's system and its relative predictive validity on organizational outcomes. *The Journal of Applied Psychology*, *104*(6), 832–850. https://doi.org/10.1037/apl0000380

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for Cybersecurity through evidence-based malware training. *Journal of Intellectual Capital, 21*(2), 203–213. https://doi.org/10.1108/JIC-05-2019-0112

Ho, F. N., Ho-Dac, N., & Huang, J. S. (2023). The effects of privacy and data breaches on consumers' online self-disclosure, Protection Behavior, and Message Valence. *SAGE Open*, *13*(3). https://doi.org/10.1177/21582440231181395

Hofkirchner, W. (2019). Social relations: Building on Ludwig von Bertalanffy. *Systems Research and Behavioral Science*, *36*(3), 263–273. https://doi.org/10.1002/sres.2594

Huyler, D., & McGill, C. M. (2019). Research design: Qualitative, quantitative, and mixed methods approach. *New Horizons in Adult Education and Human Resource Development*, *31*(3), 75–77. https://doi.org/10.1002/nha3.20258

Institutional Ethnography. (2020). In *SAGE Research Methods Foundations*. SAGE Publications Ltd.

Islam, M., Chowdhury, M., Li, H., & Hu, H. (2018). Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention. *Transportation Research Record, 2672*(19), 66–78. https://doi.org/10.1177/0361198118799012

Johnson, R. B., & Christensen, L. B. (2020). Educational research: Quantitative, qualitative, and mixed approaches, 7th ed. *Thousand Oaks*, Sage.

Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C., Xiong, P., Iqbal, S., Lamontagne, P., Ray, S., & Ghorbani, A. A. (2023). Internet of things (IOT) security dataset evolution: Challenges and future directions. *Internet of Things*, *22*, 100780. https://doi.org/10.1016/j.iot.2023.100780

Kelly, L. M., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, *13*(2), 205979912093724. https://doi.org/10.1177/2059799120937242

Kenny, R., Fischhoff, B., Davis, A., Carley, K. M., & Canfield, C. (2022). Duped by Bots: Why some are better than others at detecting fake social media personas. *Human Factors*, 0(0). https://doi.org/10.1177/00187208211072642

Kern, F. G. (2018). The trials and tribulations of applied triangulation: Weighing different data sources. *Journal of Mixed Methods Research*, *12*(2), 166–181. https://doi.org/10.1177/1558689816651032

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-Party Risk Management: A comparison of non-intrusive risk scoring reports. *Electronics*, *10*(10), 1168. https://doi.org/10.3390/electronics10101168

Kessi, S., Marks, Z., & Ramugondo, E. (2020). Decolonizing African studies. *Critical African Studies*, *12*(3), 271–282. https://doi.org/10.1080/21681392.2020.1813413

Khoda Parast, F., Sindhav, C., Nikam, S., Izadi Yekta, H., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers &Amp; Security*, *114*, 102580. https://doi.org/10.1016/j.cose.2021.102580

Kim, S., Yoon, S., Narantuya, J., & Lim, H. (2020). Secure collecting, optimizing, and deploying of firewall rules in software-defined networks. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 15166–15177. https://doi.org/10.1109/access.2020.2967503

Kipper, L. M., Iepsen, S., Dal Forno, A. J., Frozza, R., Furstenau, L., Agnes, J., & Cossul, D. (2021). Scientific mapping to identify competencies required by industry 4.0. *Technology in Society*, *64*(101454), 101454. https://doi.org/10.1016/j.techsoc.2020.101454

Kizza, J. M. (2020). *Guide to computer network security*. Springer International Publishing.

Klier, S. D., Nawrotzki, R. J., Salas-Rodríguez, N., Harten, S., Keating, C. B., & Katina, P. F. (2022). Grounding evaluation capacity development in systems theory. *Evaluation*, *28*(2), 231–251. https://doi.org/10.1177/13563890221088871

Kour, R., Karim, R., & Thaduri, A. (2020). Cybersecurity for railways – A maturity model. Proceedings of the institution of mechanical engineers, Part F: *Journal of Rail and Rapid Transit. 234(*10):1129-1148. Https://doi:10.1177/0954409719881849

Leal, M. M., & Musgrave, P. (2023). Hitting back or holding back in cyberspace: Experimental evidence regarding Americans' responses to cyberattacks. *Conflict*

Management and Peace Science, *40*(1), 42–64. https://doi.org/10.1177/07388942221111069

Lee, J.-M., & Hong, S. (2020). Keeping host sanity for security of the SCADA systems. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 62954–62968. https://doi.org/10.1109/access.2020.2983179

Leedy, P. D., Ormrod, J. E., & Johnson, L. R. (2019). Practical research: *Planning and design (12th ed.).* Pearson

Lena, Y., Michael, L., & David, S. (2019). Information security behavior: A cross-cultural comparison of Irish and US employees. *Information Systems Management 36*(2*)*, 306-322. https://doi:10.1057/s41303-017-0059-9

Levitt, H. M., Pomerville, A., Surace, F. I., & Grabowski, L. M. (2017). Metamethod study of qualitative psychotherapy research on clients' experiences: Review and recommendations. *Journal of Counseling Psychology, 64*(2), 626-644. https://doi:10.1037/cou0000222

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Libicki, M. C. (2020). The convergence of information warfare. *Information Warfare in the Age of Cyber Conflict*, 15–26. https://doi.org/10.4324/9780429470509-2

Lopez Garcia, A., De Lucas, J. M., Antonacci, M., Zu Castell, W., David, M., Hardt, M., Lloret Iglesias, L., Molto, G., Plociennik, M., Tran, V., Alic, A. S., Caballer, M., Plasencia, I. C., Costantini, A., Dlugolinsky, S., Duma, D. C., Donvito, G., Gomes, J., Heredia Cacha, I., … Wolniewicz, P. (2020). A cloud-based framework for machine learning workloads and applications. *IEEE Access, 8*, 18681–18692. https://doi.org/10.1109/access.2020.2964386

Madhuri, P., & Prabhu, E. (2023). Data protection using scrambling technique. In *Inventive Computation and Information Technologies* (pp. 811–822). Springer Nature Singapore. https://link.springer.com/chapter/10.1007/978-981-19-7402-1_58

Makin, S. (2021). The research-practice gap as a pragmatic knowledge boundary. *Information and Organization*, *31*(2), 100334. https://doi.org/10.1016/j.infoandorg.2020.100334

Mansfield-Devine, S. (2018). Friendly fire: how penetration testing can reduce your risk. *Network Security*, *2018*(6), 16–19. https://doi:10.1016/S1353-4858(18)30058-8

Mar, S. (2019). The single point of failure: The death of a CEO highlights the risks of only one person controlling access to corporate data. *Internal Auditor, 76*(2), 16-17. https://internalauditor.theiia.org/en/articles/2019/april/the-single-point-of-failure/

Marcus, D. J. (2018). The data breach dilemma: Proactive solutions for protecting consumers' Personal information. *Duke Law Journal*, *68*(3), 556–593. https://scholarship.law.duke.edu/dlj/vol68/iss3/3

Meng, X., Chen, Y., Suo, L., Xuan, Q., & Zhang, Z.-K. (Eds.). (2023). Big data and social computing: 8Th China national conference, BDSC 2023, Urumqi, China, July 15-17, 2023, proceedings (1st ed.). Springer.

Merriam, S. B. (2019). *Qualitative research in practice: Examples for discussion and analysis* (Sharan B. Merriam & R. S. Grenier, Eds.; 2nd ed.). Jossey-Bass. methods in pragmatics: Overcoming two non-fruitful dichotomies. *System*, 75, 4–12. https://doi.org/10.1016/j.system.2018.03.014

Mierzwiak, R., Xie, N., & Dong, W. (2019). Classification of Research Problems in Grey *Milbank Quarterly*, *91*(2), 459-490. https://doi:10.1111/1468-0009.12023

Miloslavskaya, N., Lima, S., & Rocha, Á. (2018). Information security management in SOCs and SICs. *Journal of Intelligent & Fuzzy Systems*, *35*(1), 2637-2647. https://doi:10.3233/JIFS-169615

Mlekus, L., Bentler, D., Paruzel, A., Kato-Beiderwieden, A.-L., & Maier, G. W. (2020). How to raise technology acceptance: user experience characteristics as technology-inherent determinants. *Gruppe Interaktion Organisation Zeitschrift Für Angewandte Organisationspsychologie (GIO)*, *51*(3), 273–283. https://doi.org/10.1007/s11612-020-00529-7

Mohammad, A. S., & Pradhan, M. R. (2021). Machine learning with big data analytics for cloud security. *Computers &Amp; Electrical Engineering*, *96*(1), 107–527. https://doi.org/10.1016/j.compeleceng.2021.107527

Monov, L. B., & Karev, M. L. (2018). Information warfare conceptual framework. *International Journal of Recent Scientific Research. 9*(5), 26859-26866. http://dx.doi.org/10.24327/ijrsr.2018.0905.2139

Motulsky, S. L. (2021). Is the member checking the gold standard of quality in qualitative research? *Qualitative Psychology (Washington, D.C.)*, *8*(3), 389–406.

https://doi.org/10.1037/qup0000215

Mthunzi, S. N., Benkhelifa, E., Bosakowski, T., Guegan, C. G., & Barhamgi, M. (2020). Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems*, *107*, 620–644. https://doi.org/10.1016/j.future.2019.11.013

Natow, R. S. (2020). The use of triangulation in qualitative studies employing elite interviews. *Qualitative Research: QR*, *20*(2), 160–173. https://doi.org/10.1177/1468794119830077

Neumann, D., & Rhodes, N. (2023). Morality in social media: A scoping review. *New Media & Society*, *0*(0). https://doi.org/10.1177/14614448231166056

Niki, O., Saira, G., Arvind, S., & Mike, D. (2022). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *Digital Health,* 8(1), 350–687 https://doi:10.1177/20552076221104665 .

Owusu-Oware, E., & Effah, J. (2022). Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation. *Information Development*, *0*(0). https://doi.org/10.1177/02666669221085709

Pacella, J. M. (2016). The cybersecurity threat: Compliance and the role of whistleblowers. *Brooklyn Journal of Corporate, Financial & Commercial Law,* *11*(1), 39–70. https://doi:10.2139/ssrn.2803995

Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with bring your own device security policies in organizations: A systematic literature review.

Computers & Security, 98. https://doi.org/10.1016/j.cose.2020.101998

Paxton, A. (2020). The Belmont Report in the age of big data: Ethics at the intersection of psychological science and data science. In *Big data in psychological research* (pp. 347–372). American Psychological Association. https://psycnet.apa.org/record/2020-39681-016

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019). Why people (don't) use password managers effectively. *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 319–338. https://www.usenix.org/conference/soups2019/presentation/pearman

Peterson, B. L., Albu, O. B., Foot, K., Hutchins, D., Qiu, J., Scott, C. R., Stohl, M., & Tracy, S. J. (2022). Conducting research in difficult, dangerous, and/or vulnerable contexts: Messy narratives from the field. *Management Communication Quarterly*, *36*(1), 174–204. https://doi.org/10.1177/08933189211058706

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pramanik, S., Sharma, A., Bhatia, S., & Le, D.-N. (2022). *An interdisciplinary approach to modern network security* (1st Edition). CRC Press. https://doi.org/10.1201/9781003147176

Prasad, A., & Chandra, S. (2023). Machine learning to combat cyberattack: a survey of datasets and challenges. *The Journal of Defense Modeling and Simulation. 20*(4), 577-588. https://doi:10.1177/15485129221094881

Primack, B. A., Karim, S. A., Shensa, A., Bowman, N., Knight, J., & Sidani, J. E. (2019). Positive and negative experiences on social media and perceived social isolation. *American Journal of Health Promotion.* 33(6):859-868. https://doi:10.1177/0890117118824196

Pritchard, I. A. (2021). Framework for the ethical conduct of research: The ethical principles of the Belmont Report. In *Handbook of research ethics in psychological science* (pp. 3–21). American Psychological Association. https://psycnet.apa.org/record/2021-62614-001

Purkait, S., & Damle, M. (2023). Cyber security and frameworks: A study of cyber-attacks and methods of prevention of cyber-attacks. *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. https://ieeexplore.ieee.org/document/10104823

Quintão, C., Andrade, P., & Almeida, F. (2020). How to improve the validity and reliability of a case study approach? *Journal of Interdisciplinary Studies in Education*, *9*(2), 273–284. https://doi.org/10.32674/jise.v9i2.2026

Rahim, N. H. A., Hamid, S., & Kiah, L. M. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An Assessment. *Malaysian Journal of Computer Science*, *32*(3), 221-245. https://doi:10.22452/mjcs.vol32no3.4

Rakas, S. V. B., Stojanovic, M. D., & Markovic-Petrovic, J. D. (2020). A review of research work on network-based SCADA intrusion detection systems. *IEEE*

Access: Practical Innovations, Open Solutions, *8*, 93083–93108. https://doi.org/10.1109/access.2020.2994961

Ravikumar, K. C., Chiranjeevi, P., Manikanda Devarajan, N., Kaur, C., & Taloba, A. I. (2022). Challenges in internet of things towards the security using Deep Learning Techniques. *Measurement: Sensors*, *24*, 100473. https://doi.org/10.1016/j.measen.2022.100473

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open, 11*(1). https://doi.org/10.1177/21582440211000049

Rice, R. M. (2021). High-Reliability Collaborations: Theorizing inter-organizational reliability as constituted through translation. *Management Communication Quarterly*, *35*(4), 471–496. https://doi.org/10.1177/08933189211006390

Ridder, H. (2020). The theory contribution of case study research designs. *Business Research, 10, 281-30.* https://link.springer.com/article/10.1007/s40685-017-0045-z

Rostami, E., Karlsson, F., & Gao, S. (2020). Requirements for computerized tools to design information security policies. *Computers & Security, 99*. https://doi.org/10.1016/j.cose.2020.102063

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Scott, A. L., Howe, W. T., & Bisel, R. (2023). Reviewing high reliability team (HRT) scholarship: A 21st century approach to safety. *Small Group Research*, *54*(1), 3–

40. https://doi.org/10.1177/10464964221116349

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, *97*(101996), 101996. https://doi.org/10.1016/j.cose.2020.101996

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers &Amp; Security*, *124*, 102974. https://doi.org/10.1016/j.cose.2022.102974

Shields, T., Li, H., Lebedev, P., & Dykstra, J. (2020). Cyber Buzz: Examining virality characteristics of cybersecurity content in social networks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *64*(1), 441–445. https://doi.org/10.1177/1071181320641099

Shlomo, A., Kalech, M., & Moskovitch, R. (2021). Temporal pattern-based malicious activity detection in SCADA systems. *Computers & Security*, *102*(102153), 102153. https://doi.org/10.1016/j.cose.2020.102153

Sim, J. H. (2020). Moving towards a mixed-method approach to educational assessments. *Academic Medicine*, *92*(6), 726–726. https://doi.org/10.1097/acm.0000000000001680

Simola, S. (2018). Fostering collective growth and vitality following acts of moral courage: A general system, relational psychodynamic perspective*. Journal of Business Ethics, 148*(1), 169–182. https://doi.org/10.1007/s10551-016-3014-0

Singh, N., Benmamoun, M., Meyr, E., & Arikan, R. H. (2021). Verifying rigor: analyzing qualitative research in international marketing. *International Marketing Review, 38*(6), 1289–1307. https://doi.org/10.1108/imr-03-2020-0040

Slepian, M. L., & Jacoby-Senghor, D. S. (2021). Identity threats in everyday life: Distinguishing belonging from inclusion. *Social Psychological and Personality Science*, *12*(3), 392–406. https://doi.org/10.1177/1948550619895008

Soomro, K. A., Kale, U., Curtis, R., Akcaoglu, M., & Bernstein, M. (2020). Digital divide among higher education faculty. *International Journal of Educational Technology in Higher Education*, *17*(1). https://doi.org/10.1186/s41239-020-00191-5

Sun, J. (2022). Computer network security technology and prevention strategy analysis. *Procedia Computer Science*, *208*, 570–576. https://doi.org/10.1016/j.procs.2022.10.079

Susanto, H., Fang Yie, L., Mohiddin, F., Rahman Setiawan, A. A., Haghi, P. K., & Setiana, D. (2021). Revealing social media phenomenon in time of COVID-19 pandemic for boosting start-up businesses through digital ecosystem. *Applied System Innovation*, *4*(1), 6. https://doi.org/10.3390/asi4010006

Taguchi, N. (2018). Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research. *System, 75*, 23–32. https://doi.org/10.1016/j.system.2018.03.010

Tahir, R. (2018). A study on malware and malware detection techniques. *International Journal of Education and Management Engineering*, *8*(2), 20–30. https://doi.org/10.5815/ijeme.2018.02.03

Tan, X., & Yu, F. (2018). Research and application of virtual user context information security strategy based on group intelligent computing. *Cognitive Systems Research. 52*(2), 629-639. https://doi:10.1016/j.cogsys.2018.08.016

Tao, X., Kong, K., Zhao, F., Cheng, S., & Wang, S. (2020). An efficient method for network security situation assessment. *International Journal of Distributed Sensor Networks*, *16*(11), 155014772097151. https://doi.org/10.1177/1550147720971517

Tayaksi, C., Ada, E., Kazancoglu, Y., & Sagnak, M. (2022). The financial impacts of information systems security breaches on publicly traded companies: Reactions of different sectors, *Journal of Enterprise Information Management*, *35*(2), 650-668. https://doi.org/10.1108/JEIM-11-2020-0450

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. *Perioperative nursing*, 7(3), 155-163. http://doi.org/10.5281/zenodo.2552022

ThiBac, D., & Minh, N. H. (2022). Design of network security storage system based on under cloud computing technology. *Computers and Electrical Engineering*, *103*, 108334. https://doi.org/10.1016/j.compeleceng.2022.108334

Thimm, H. (2022). Systems theory-based abstractions and decision schemes for corporate environmental compliance management. *Sustainable Operations and Computers*, *3*, 188–202. https://doi.org/10.1016/j.susoc.2022.01.007

Tornblad, M. K., Jones, K. S., Namin, A. S., & Choi, J. (2021). Characteristics that predict phishing susceptibility: A Review. *Proceedings of the Human Factors and*

Ergonomics Society Annual Meeting, *65*(1), 938–942. https://doi.org/10.1177/1071181321651330

Trumbach, C. C., Payne, D. M., & Walsh, K. (2023). Cybersecurity in business education: The ‘how to’ in incorporating education into practice. *Industry and Higher Education*, *37*(1), 35–45. https://doi.org/10.1177/09504222221099389

Tsaregorodtsev, A. V., Lvovich, I. Y., Shikhaliev, M. S., Zelenina, A. N., & Choporov, O. N. (2019). Information security management for cloud infrastructure. *International Journal on Information Technologies & Security*, *11*(2), 91-100. https://ijits-bg.com/contents/IJITS-No3-2019/2019-N3-09

Vanderstraeten, R. (2019). Systems everywhere? *Systems Research and Behavioral Science*, *36*(3), 255–262. https://doi.org/10.1002/sres.2596

Verma, A., & Shri, C. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision*, *0*(0). https://doi.org/10.1177/09722629221074760

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*(1), 2172–2175. https://doi.org/10.1016/j.matpr.2021.11.121

Walden University. (2023). Office of Research and Doctoral Studies: DBA capstone studies. https://academicguides.waldenu.edu/research-center/program-documents/dba

Werder, K., & Maedche, A. (2018). Explaining the emergence of team agility: A complex adaptive systems perspective. *Information Technology & People*, *31*(3), 819-844. https://doi.org/10.1108/ITP-04-2017-0125

White, P., & Forrester-Jones, R. (2020). Valuing e-inclusion: social media and the social networks of adolescents with intellectual disability. *Journal of Intellectual Disabilities*, *24*(3), 381–397. https://doi.org/10.1177/1744629518821240

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage.

Whyte, J. (2022). Cybersecurity, race, and the politics of truth. *Security Dialogue, 53*(4), 342–362. https://doi.org/10.1177/09670106221101725

Wu, Q., Li, Q., Guo, D., & Meng, X. (2022). Exploring the vulnerability in the inference phase of advanced persistent threats. *International Journal of Distributed Sensor Networks*, *18*(3), 155013292210804. https://doi.org/10.1177/15501329221080417

Xiong, W., & Lagerström, R. (2019). Threat modeling: A systematic literature review. *Computers & Security*, *84*(2), 53-69. https://doi:10.1016/j.cose.2019.03.010

Y. Connolly, L., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomizing countermeasures. *Computers & Security*, *87*(101568), 101568. https://doi.org/10.1016/j.cose.2019.101568

Yin, R. (2018). *Case study research: Design and methods* (6Th ed.). Sage.

Yu, S. (2020). Crime hidden in email spam. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 851–863). IGI Global. https://doi.org/10.4018/978-1-5225-9715-5.ch057

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, *56*(4), 570–601. https://doi.org/10.1016/j.im.2018.10.001

Zenker, S., & Kock, F. (2020). The coronavirus pandemic – A critical discussion of a tourism research agenda. *Tourism Management, 81*(104164), 104164. https://doi.org/10.1016/j.tourman.2020.104164

Zhao, Y., Zhu, F., Zhang, W., & Su, H. (2023). Security switching control of the cyber-physical system with incremental quadratic constraints under a denial-of-service attack. *Transactions of the Institute of Measurement and Control. 45*(1):157-167. https://doi:10.1177/01423312221105141

Zhu, Z. (2022). Paradigm, specialty, pragmatism: Kuhn's legacy to methodological pluralism. *Systems Research and Behavioral Science*, *39*(5), 895–912. https://doi.org/10.1002/sres.2881

Appendix: Interview Protocol

Date______________________ Time____________

Interviewer:

Participant Pseudonym:

Set up electronic equipment before interviewing the participant.

Begin introductions: My name is Rene Ekoteson. Thank you for participating in this interview. I will be facilitating this interview. Today's date is (state the date).

Purpose of the interview: This interview aims to identify and explore the effective strategies IT leaders of universities in Cameroon use to prevent or mitigate cyberattacks' costs. There are no right or wrong answers.

Remind the participant that their identity is anonymous. I will assign you a code to conceal your identity. You can find the code at the top of your consent form. I will refer you by your code for the remainder of the interview.

Get permission to record the interview: With your permission, I would like to audiotape the interview. The objective of recording the interview is to ensure I capture all your responses accurately.

Explain member checking to the participant: I will contact you within one week to provide a transcribed copy of my notes to ensure I captured all your responses accurately. At that time, you will have one day to review the transcribed data collected during the interview. I will follow up by phone to check the information with you and to answer any questions.

Assure the participant that their information will be confidential: I assure you that all your comments will remain confidential. I will be compiling data containing all participants' comments without any reference to individuals.

Review the consent form and have the participant acknowledge their consent

Collect a signed copy of the consent form:

Before the interview, you received a consent form. Please keep one for your copy, and I will keep the signed document.

Check the folder for a signed consent form. Acknowledge if I do not have the signed consent form. If I do not have the consent form, ask the participant, did you bring your consent letter? If not, I have one here for you. (Copies distributed). Do you have any questions?

Explain the duration of the interview: The interview will take approximately 40 to 60 minutes and will follow an interview protocol. There will be no incentives for participating in this interview.

If you are ready, let us begin with some background questions.

1. Is your institution accredited by the Cameroon Ministry of Higher Education? **YES /NO**
2. Are you a security manager in your institution? **YES / NO**
3. Have you used effective strategies to prevent cyberattacks? **YES /NO**
4. Do you have over five years of experience in cybersecurity management? **YES /NO**
5. Are you more than 25 years of age? **YES /NO**

Let us begin with the research question.

1. What strategies do you use to prevent cyberattacks in your institution?
2. How effective or successful are these strategies?
3. What challenges do you encounter implementing these Strategies?
4. What training do you have for your staff and students to fight against cyberattacks?
5. What policies and procedures have you adopted to address cyberattacks in your institution?
6. What additional information would you like to share regarding your strategies to prevent cyberattacks in your institution?
7. Is there anything else you would like to add?

Conclude interview. This concludes the interview. Thank you for participating. You will receive a transcribed copy of my notes within one week from today.